RECEIVER-INDEPENDENT SPOOFING DETECTION DEVICE

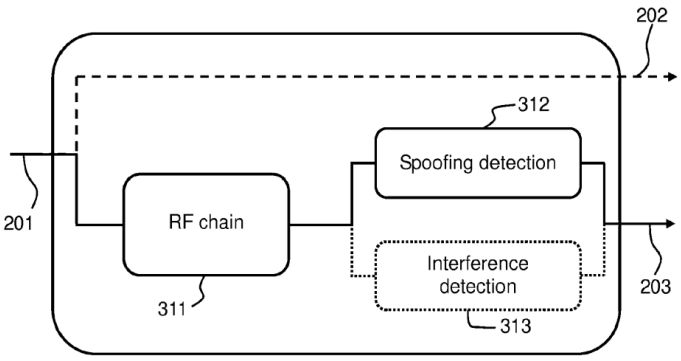
Technological advantages

Innovative :

- Use a dedicated device to compute cross correlation functions to validate proper GNSS signals.

Efficient :

- Does not require extensive memory or computing power.
- No change in the GNSS receiver core processing.



Schematic of a spoofing detection device

(201) Input satellite GNSS signals
(202) Output GNSS signals
(203) Information about spoofing
(311) RF chain for signal conversion
(312) Computer logic (compute cross-correlation functions)
(313) Interference detection module

Invention synthesis

The invention deals with GNSS receivers positioning and signal spoofing.
GNSS receivers used in civilian applications are unprotected and open to malicious attacks. Military grade GNSS signals have some degrees of encryption but are still vulnerable, also encryption is costly. While obvious attacks (sudden changes) can be easily spotted, spoofing using meaconing or gradual insidious changes are difficult to counter.
The invention is based on acquiring and digitalizing GNSS signals containing a navigation message modulated by a spreading code. Cross correlation functions are computed over a grid of spreading code phase delay and Doppler shifts, between the signal and locally generated signal replicas. From the cross-correlation peaks, it is then possible to identify spoofing.

Commercial benefits

- Protection of GNSS receivers against malicious attacks.
- Ensures the safe operation of critical services based on GNSS uses.

Potential applications

- All GNSS positioning receivers and all constellations.

Patented invention - under license.

For more information :

Valo-TT@cnes.fr