DEVICE AND METHOD TO DETECT SPOOFING OF A TERMINAL

Technological advantages

Innovative :

- Use of a non-GNSS signal to validate the correctness of GNSS signals.
- Only requires a link to a server or to RF based items (Wi-Fi, Bluetooth, RFID…).

Efficient :

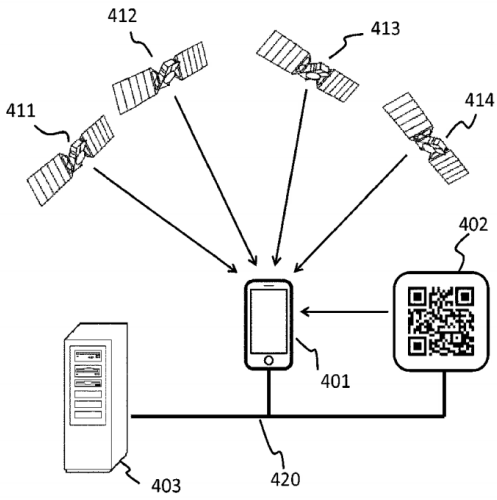
- Encryption of the non-GNSS signal guarantees the validity of the original GNSS signals.
- May detect small insidious alterations.

Invention synthesis

The invention deals with the detection of spoofing and discrepancies in a positioning receiver, especially dealing with GNSS signals.
It is known that civilian GNSS signals are easy to spoof, distort or block. Military GNSS signals have a low level cryptographic authentication and are still prone to meaconing. Encrypted satellite signals are costly. While detection of strong and rapid discrepancies can be easy, slow and insidious changes are difficult to counter.
The invention implements a two-factors validation. The terminal gets and compare information from GNSS signals (pseudo-range, navigation message, time, …) and from an encrypted non-GNSS type signal (optical, RF) relative to a position.

Potential applications

- Telecommunications, electrical power supplies, banks, finance, …



Schematic based on this invention applied to GNSS signals

(401) Terminal for positioning calculation
(402) Optical display
(403) Server
(420) Data link
(411,412,413,414) GNSS signal emitters

Commercial benefits

- Two-factors validation method. Enhanced security at low cost, simple to set-up and deploy.

Patented invention - under license.

For more information :

Valo-TT@cnes.fr