DISPOSITIF ET MÉTHODE DE DÉTECTION D'USURPATION POUR UN TERMINAL

Avantages technologiques

Innovant :

- Utilisation d'un signal non-GNSS pour valider la légitimité d'un signal GNSS.
- Ne demande qu'un lien à un serveur ou à un moyen RF (Wi-Fi, Bluetooth, RFID…).

Performant :

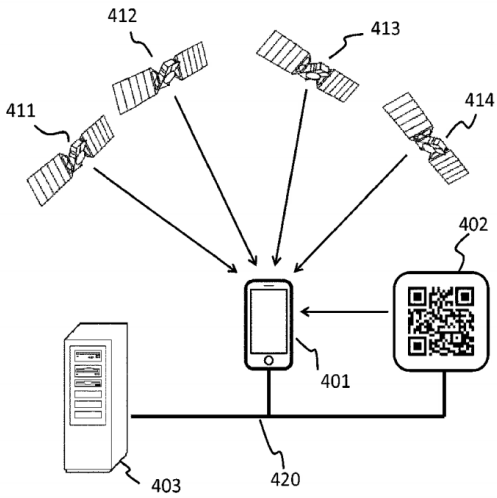
- La cryptographie du signal non-GNSS garantie la validité du signal GNSS originel.
- Permet de détecter les altérations légères et insidieuses.

Synthèse de l'invention

L'invention présente un système de détection d'usurpation et de manipulation d'un récepteur de positionnement, en particulier de type GNSS.
Il est connu que les signaux GNSS sont facilement manipulables, falsifiables voir bloqués. Les signaux GNSS militaires ont un degré de cryptographie qui reste attaquable notamment en termes de transplexion. L'utilisation de cryptographie bord satellite est couteuse. Les changements rapides et violents dans la nature des signaux sont facilement repérables, les modifications légères et insidieuses sont elles difficiles à contrer.
L'invention implémente une validation à deux-facteurs. Le terminal acquière et compare les informations des signaux GNSS (pseudo-distance, message, temps…) et les informations d'un signal crypté non-GNSS (optique, RF) indiquant un positionnement.

Applications potentielles

- Télécommunications, alimentations électriques, banques, finance, …



Vue schématique d'une application basée sur l'invention

(401) Terminal pour le calcul de position
(402) Affichage optique
(403) Serveur
(420) Lien de données
(411,412,413,414) Emetteurs GNSS

Bénéfices commerciaux

- Méthode de validation à deux-facteurs. Amélioration à bas coût de la sécurité, simple à mettre en œuvre et à déployer.

Invention brevetée disponible sous licence.

Pour en savoir +

Valo-TT@cnes.fr