UNITÉ DE DÉTECTION D'USURPATION INDÉPENDANTE D'UN TERMINAL

Avantages technologiques

Innovant :

- Utilisation d'une unité dédiée de calcul de fonctions de corrélations croisées pour valider un signal.

Performant :

- Ne demande pas de puissance de calcul ou de mémoire élevées.
- Pas de changement dans le cœur du traitement des signaux pour un récepteur GNSS.

Synthèse de l'invention

L'invention concerne les récepteurs GNSS et en particulier l'usurpation de signaux.
Les récepteurs GNSS utilisés dans les applications civiles sont non-protégés et vulnérables aux attaques. Les signaux GNSS dans le domaine militaire ont un niveau de cryptage mais qui reste vulnérable, l'encodage étant couteux et complexe à mettre en œuvre. Les attaques brutes (changements soudains) peuvent être facilement détectées alors que l'usurpation de signaux utilisant la transplexion ou les changements graduels insidieux sont difficiles à contrer.
L'invention se base sur l'acquisition et la numérisation de signaux GNSS contenant un message modulé par un code d'étalement. Les fonctions de corrélations croisées sont calculées sur une matrice de code d'étalement en retard de phase et de déplacement Doppler, entre le signal d'origine et les répliques localement générées. A partir des pics de corrélation, il est possible de détecter les usurpations.

Applications potentielles

- Toutes constellation GNSS et tous récepteurs GNSS.

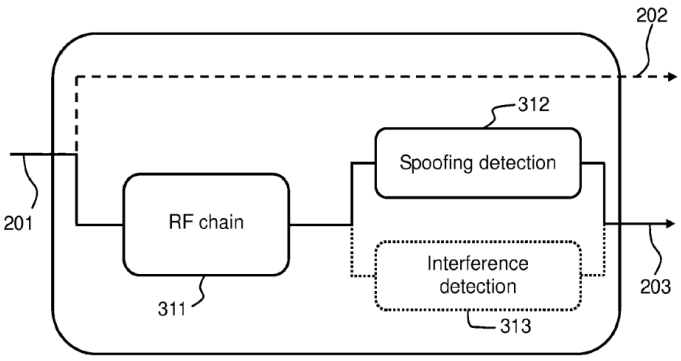

Schéma d'une unité de détection d'usurpation

(201) Données d'entrée du satellite
(202) Données de sortie
(203) Information sur l'usurpation
(311) Module RF pour la conversion du signal (numérisation)
(312) Unité de calcul des fonctions de corrélations croisées
(313) Module de détection d'interférence

Bénéfices commerciaux

- Protection des récepteurs GNSS contre les attaques malicieuses.
- Garanti le fonctionnement correct de services critiques basés sur les signaux GNSS.

Invention brevetée disponible sous licence.