Télécoms, navigation

POSITIONNEMENT CRYPTÉ ANTI-LEURRAGE / ANTI -SPPOFING

Systène innovant de positionnement sécurisé pour un groupe d'utilisateurs

Avantages technologiques

Sécurisation et garantie d'authentification de la localisation

Garantie d'authentification par le GNSS
Possibilité pour un terminal de devenir un serveur (basculer d'une PVT attaquée vers une solution sécurisée (cryptage)

Une solution plus compacte, plus légère

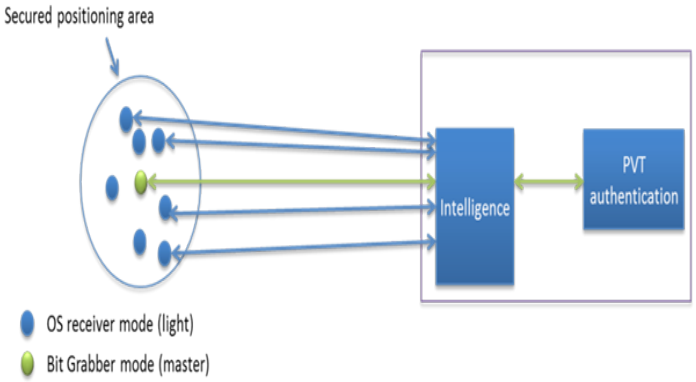
1 seul récepteur sécurisé (grabber) pour sécuriser l'ensemble
Possibilité d'avoir des terminaux light (pas que des grabber)
Adaptation de la qualité de l'intelligence dans le serveur et dans les terminaux

Une efficacité renforcée en cas d'attaque

Détection des attaques
Communication directe des terminaux utilisateurs entre eux possible
Données brutes au lieu de PVT garantie l'authentification

Synthèse de l'invention

Nouvelle méthode basée sur une vérification délocalisée de l'authenticité des signaux GNSS par un centre d'authentification. Le centre d'authentification (partie droite du graphique) vérifie l'authenticité des signaux GNSS reçus par des récepteurs d'utilisateurs. Cette vérification permet de détecter la tentative de leurrage et de localiser la source suspecte



Bénéfices commerciaux

Filtrage / Identification

Coût moindre car un seul émetteur-récepteur sécurisé par groupe d'intervention

Moins de pertes (matériel, humain…)

Meilleure efficacité sur le terrain

Intervention tout-terrain

Applications potentielles

Armée, Police
Garde-côtes, flottes
Douanes, services spéciaux, gestion de flotte critique
Tout type de groupes

TRL : 9

Invention patented by CNES

Pour en savoir plus :

CNES Valorisation :
+33 (0) 5 61 27 39 00
valorisation@cnes.fr