Régis DELEPINE

Spoofing GPS :
Relever les défis du brouillage et de l'usurpation GPS

Promotion 2024-2025

Résumé

Spoofing GPS, un terme inexistant il y a 10 ans dans le langage commun, s’impose de plus en plus dans notre vie de tous les jours et lors des opérations terrestre, aérienne et maritime civiles et militaires.

A la différence du brouillage, l’usurpation ou spoofing GPS est plus insidieuse donc plus dangereuse. Elle amène souvent à une incompréhension de la situation qui peuvent être dangereux pour les individus et la société.

le spoofing GPS soulève plusieurs préoccupations. Il est souvent utilisé de manière malveillante, par exemple pour tromper les systèmes de navigation des véhicules, des drones, ou même des avions, ce qui peut avoir des conséquences graves sur la sécurité. Dans le domaine des jeux vidéo a réalité augmenté, il permet aux joueurs de tricher en simulant un déplacement vers des lieux où se trouvent des objets ou des créatures virtuelles rares, ce qui va à l'encontre des règles établies par les développeurs.

Le spoofing GPS pose également des défis en matière de cybersécurité et de confidentialité. Les individus et les organisations doivent être conscients des risques potentiels et prendre des mesures pour se protéger contre de telles attaques, comme l'utilisation de systèmes de navigation complémentaires et la mise à jour régulière des logiciels.

En conclusion, bien que le spoofing GPS puisse sembler être une simple manipulation technique, ses implications sociales et éthiques sont vastes, affectant la sécurité, l'équité et la confidentialité dans beaucoup de domaines.

Les naufrageurs

1. Introduction

Les systèmes globaux de navigation par satellite tel le GPS, mais aussi Galileo, GLONASS et Beidou représentent une infrastructure primordiale pour notre société. Ils ont pour but de fournir à l'utilisateur une information précise de position, de vitesse et de temps, à tout instant, en tout lieu et dans n'importe quelles conditions atmosphériques du globe. Nous obtenons ainsi une couverture quasi mondiale et quasi permanente, une précision de localisation très importante et un nombre d'utilisateurs illimités avec un coût très faible du service.

Le GPS est un système assez complexe composé de 31 satellites, d'un certain nombre de stations de surveillance et d'un centre de contrôle. Des milliards de récepteurs GPS représentent le segment utilisateur. Ces récepteurs et les stations de surveillance reçoivent un signal radio satellite faible et sont donc sensibles à des interférences telles que le brouillage ou l'usurpation d'identité.

Le spoofing ou usurpation GPS est une technique par laquelle des signaux GPS sont falsifiés pour tromper un récepteur GPS sur sa position réelle. Cette technologie, bien que complexe, a des implications profondes dans divers domaines, notamment la sécurité, la navigation et la défense. Dans un monde de plus en plus dépendant des systèmes de positionnement global, comprendre les enjeux du spoofing GPS devient crucial.

Cette étude vise à explorer les dimensions techniques du spoofing GPS tout en mettant l'accent sur ses impacts sociaux, éthiques et juridiques, offrant ainsi une large perspective pour les sciences humaines et sociales [1].

[1]. http://webriviere.free.fr/sciences/rapports/expose/tempsfreq.pdf

2. Contexte et Fondements Théoriques

Le spoofing GPS implique la création de signaux GPS contrefaits qui imitent les signaux réels émis par les satellites GPS. Les récepteurs GPS, non protégés par conception, ne peuvent distinguer les signaux authentiques des signaux falsifiés et calculent une position incorrecte.

Cette technique peut être utilisée pour induire en erreur les systèmes de navigation des véhicules terrestres, maritimes et aériens ainsi que les infrastructures critiques dépendantes du GPS pour leur synchronisation.

Les premières tentatives de brouillage et de manipulation des signaux de navigation remontent à plusieurs siècles avec l'exemple des naufrageurs. Les réalités de l'histoire ainsi que les contes et légendes parlent des naufrageurs des 17éme et 18éme siècle. Il consistait à allumer de faux feux sur la côte pendant les nuits de tempête pour induire en erreur les navires en détresse. Pensant qu'ils étaient proches d'un port sûr, les capitaines échouaient leurs navires sur les récifs, où ils se brisaient [2].

Initialement développé à des fins militaires, le spoofing GPS est devenu plus accessible avec l'avancement des technologies de l'information. Aujourd'hui, des kits de spoofing GPS peuvent être trouvés sur web.

Exemple : GPS Spoofing, contrôlez la localisation de votre téléphone Android [3]

Dans le contexte des sciences humaines et sociales, le spoofing GPS soulève des questions sur la confiance dans la technologie, la vulnérabilité des infrastructures modernes, et les implications pour la vie privée et la sécurité.

[2]. Letemps1biere. (2025, 23 janvier). Qui étaient les naufrageurs ? - Le temps d& # 039 ; une bière. *Le Temps d'une Bière*. https://letempsdunebiere.ca/ggaspesie-terre-naufrageurs/

[3]. Android MT. (2021, 17 octobre). *Tuto Express : GPS Spoofing, contrôlez la localisation de votre tel Android* [Vidéo]. YouTube. https://www.youtube.com/watch?v=DLOB0nn-kgE

3. Impact Social et Éthique

Impact Social

- **Sécurité Publique** :

  L'industrie actuelle utilise la localisation de précision. Elle peut être utilisée comme un outil d'optimisation des flux de production ou des opérations de maintenance et d'arrêts techniques en permettant une gestion efficace des équipements sur un site industriel. Grâce aux systèmes de localisation, il est possible de suivre en temps réel la position des machines, des outils, des pièces dans le flux de production ou encore des véhicules ou des robots autonomes. La problématique du brouillage ou de l'usurpation GPS prend dans ce domaine toute son ampleur [4].

  Dans les transports, l'usurpation GPS peut perturber les systèmes de navigation utilisés par les avions, les navires et les véhicules, ce qui peut entraîner des accidents et des retards [5].

  Les infrastructures critiques, telles que les réseaux électriques et les systèmes de communication, dépendent souvent du GPS pour leur synchronisation.

  La liste de ces services essentiels en France correspond à onze secteurs : l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, les services fournis par l'administration publique, le secteur de l'espace, le secteur de la production, transformation et distribution de denrées alimentaires. Leur destruction ou leur perturbation aurait en effet un impact important pour le pays ou une entreprise.

  Le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen vise à garantir que les services essentiels au maintien des fonctions sociétales vitales ou des activités économiques soient fournis sans entrave dans le marché intérieur et que la résilience des entités critiques fournissant ces services soit renforcée [6] [7] [8] [9].

  [4]. Gilbert, J., & Gilbert, J. (2024, 31 octobre). *La localisation de précision au service de l'industrie 4.0*. Sysnav | High Precision Positioning For Critical Decisions. https://www.sysnav.fr/localisation-de-precision-au-service-de-lindustrie40/

  [5]. OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024, 6 septembre). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP. https://ops.group/blog/gps-spoofing-final-report/

[6] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302450

[7] https://www.areion24.news/2023/10/23/la-securite-des-communications-par-satellite-une-infrastructure-critique-pour-la-transmission-de-donnees

[8] https://www.areion24.news/2023/10/23/la-securite-des-communications-par-satellite-une-infrastructure-critique-pour-la-transmission-de-donnees

[9] https://www.electronicspecifier.com/news/analysis/uk-consumers-are-concerned-about-the-risk-of-gps-spoofing

- **Confiance dans la Technologie** :

  La dépendance technologique au GPS est devenue omniprésente dans de nombreux aspects de la vie moderne. Voici quelques domaines clés où cette dépendance est particulièrement marquée :

  L'agriculture de précision utilise le GPS pour optimiser les pratiques agricoles, comme les plantations, l'irrigation et les récoltes, améliorant ainsi l'efficacité et réduisant les coûts.

  De nombreuses applications mobiles basés sur la localisation, comme les services de cartographie, les applications de fitness, les services de livraison de nourriture et les réseaux sociaux, utilisent le GPS pour fournir des services basés sur la localisation.

  Les systèmes de navigation GPS sont largement utilisés dans les voitures, les camions et les motos pour le guidage routier et la gestion du trafic. Les avions utilisent le GPS pour la navigation aérienne, l'atterrissage et la gestion du trafic aérien. Les navires dépendent du GPS pour la navigation en mer, la sécurité et la gestion des routes maritimes [10].

  Logistique et Transport de Marchandises : le suivi des expéditions et la gestion des flottes de véhicules de livraison reposent fortement sur les technologies GPS pour l'optimisation des itinéraires et le suivi en temps réel.

  Les services d'urgence utilisent le GPS pour localiser les appels de détresse et envoyer des secours rapidement. Les systèmes de sécurité personnels et les dispositifs de suivi pour enfants et personnes âgées dépendent également du GPS.

  Synchronisation des réseaux : les réseaux de communication et les systèmes informatiques utilisent souvent des signaux GPS pour la synchronisation précise du temps, ce qui est crucial pour les transactions financières et les opérations de réseau.

  En somme, bien que le GPS ait révolutionné de nombreux aspects de la vie moderne, cette dépendance technologique nécessite une gestion prudente pour atténuer les risques potentiels.

  [10] http://scripties.hzs.be/Repository/Eindwerk_Definitief_2618_1670079390.pdf

- **Risques et Défis**

  Désinformation : le spoofing GPS peut être utilisé pour diffuser de fausses informations de localisation, ce qui peut semer la confusion et la méfiance parmi les utilisateurs de technologies de navigation [11].

  Exploitation criminelle : une application criminelle courante est la manipulation des systèmes de repérage des véhicules. Les voleurs utilisent l'usurpation GPS pour masquer la localisation réelle des véhicules volés, ce qui complique l'action des forces de police. De même, les passeurs utilisent ces techniques pour dissimuler les itinéraires de leurs envois illégaux, en soustrayant la détection par les autorités chargées du contrôle des frontières et des douanes. Il y a également eu des cas d'usurpation GPS utilisé pour contourner les restrictions géographiques sur les services en ligne ou pour falsifier les données de localisation dans des applications qui offrent des récompenses ou des avantages basés sur la localisation.

  Manipulation des jeux et des divertissements : l'industrie du jeu et du divertissement a vu une augmentation de l'usurpation de GPS, principalement comme un moyen pour les joueurs d'obtenir des avantages dans les jeux et les applications basés sur la localisation. Les jeux de réalité augmentée qui s'appuient sur des sites du monde réel sont devenus des cibles pour les joueurs qui cherchent à tromper le système. En utilisant des techniques d'usurpation GPS, certains joueurs peuvent faire apparaître leurs appareils à différents endroits, ce qui leur permet d'accéder aux fonctionnalités du jeu ou de collecter des éléments virtuels sans voyager physiquement. Cela permet non seulement de perturber l'expérience de jeu prévue, mais peut également conduire à des avantages indubitables dans les aspects de la compétition de ces jeux [12].

  Ce comportement pose d'importants défis aux développeurs de jeux et aux éditeurs. Ils doivent constamment mettre à jour leurs systèmes pour détecter et prévenir l'usurpation du GPS, le maintien du fair-play et l'intégrité de leurs jeux [13].

  Vie Privée :

  Surveillance et Traçage : Ces dernières années ont vu se développer des contentieux relatif au respect de la vie privée dans les relations de travail. Le contexte d'une tension entre d'une part, l'exercice de l'autorité patronale au travers d'une surveillance du travailleur et d'autre part, le droit de ce dernier au respect de la vie privée. Le spoofing GPS peut être utilisé pour manipuler les systèmes de surveillance et de traçage, ce qui pose question sur la vie privée et la protection des données personnelles [14] [15].

  Le placement sous surveillance électronique mobile (PSEM) ou bracelet électronique GPS permet pour certaines peines de prison de suivre l'individu dans le cadre de la libération conditionnelle et du suivi socio-judiciaire [16] .

« Spoofer » le signal GPS de son bracelet électronique peut avoir des conséquence grave pour la société [17].

[11] https://www.uber.com/es/en/drive/driver-app/fraud- activities/

[12] Guy, A. R. (2024, 15 juin). *Exploring the Ethics of Pokemon Go Location Spoofing*. PrivacyPortal. https://www.privacyportal.co.uk/blogs/free-rooting-tips-and-tricks/exploring-the-ethics-of-pokemon-go-location-spoofing

[13] Caesar, J. (2024, 16 décembre). *What Is GPS Spoofing ? A Look at Its Risks and Solutions*. Tech Review Advisor. https://techreviewadvisor.com/what-is-gps-spoofing/

[14] https://pure.unamur.be/ws/portalfiles/portal/51733550/8627.pdf

[15] Guy, A. R. (2024b, juin 15). *Exploring the Ethics of Pokemon Go Location Spoofing*. PrivacyPortal. https://www.privacyportal.co.uk/blogs/free-rooting-tips-and-tricks/exploring-the-ethics-of-pokemon-go-location-spoofing

[16] *Définition - Placement sous surveillance électronique mobile / PSEM / PSEM | Insee*. (s. d.). https://www.insee.fr/fr/metadonnees/definition/c1833

[17] https://www.leparisien.fr/archives/des-ondes-pour-brouiller-les-pistes-13-05-2015-4766283.ph

Sécurité Individuelle :

Le fait de tromper un récepteur GPS en lui envoyant de faux signaux, peut avoir plusieurs impacts sur la sécurité individuelle. Un véhicule ou une personne peut être orienté vers une zone dangereuse ou créer un accident. Les applications de sécurité qui utilisent le GPS pour suivre la position d'une personne (comme les applications de suivi pour enfants ou personnes âgées) peuvent être compromises, rendant difficile la localisation de la personne en cas d'urgence [18] .

[18] *Un yacht piraté en détournant le signal GPS*. (s. d.-b). LeMondeInformatique. https://www.lemondeinformatique.fr/actualites/lire-un-yacht-pirate-en-detournant-le-signal-gps-54563.html

Impact Éthique

Le spoofing GPS peut faciliter la surveillance non autorisée, notamment par des gouvernements ou des acteurs malveillants. Cela soulève des questions éthiques concernant la collecte et l'utilisation des données de localisation sans consentement explicite, compromettant ainsi la confidentialité des individus. Des recherches en santé publique en Inde et au Pérou ont mis en évidence ce risques de ré-identification spatiale et les défis liés à la confidentialité des données géospatiales [19].

Le spoofing GPS est parfois utilisé par les employés pour contourner des systèmes de surveillance perçus comme intrusifs. Cela soulève des questions éthiques sur la vie privée des employés, la transparence des employeurs et la confiance au sein des organisations [20].

L'utilisation des données de localisation peut entraîner des discriminations, par exemple, en influençant les primes d'assurance ou en facilitant le profilage des individus. Ces pratiques

soulèvent des préoccupations éthiques concernant l'équité et la protection des droits des individus [21].

Le spoofing GPS peut être utilisé à des fins malveillantes, comme le vol de données ou la perturbation des services publics. Cependant, il peut également être utilisé pour des tests de sécurité et des recherches académiques. La ligne entre l'usage éthique et non éthique est souvent floue. Les développeurs et les utilisateurs de technologies de spoofing doivent être conscients des implications éthiques de leurs actions et prendre des mesures pour prévenir les abus [22] [23].

[19] Apte, A., Ingole, V., Lele, P., Marsh, A., Bhattacharjee, T., Hirve, S., Campbell, H., Nair, H., Chan, S., & Juvekar, S. (2019). Ethical considerations in the use of GPS-based movement tracking in health research – lessons from a care-seeking study in rural west India. *Journal Of Global Health*, *9*(1). https://doi.org/10.7189/jogh.09.010323

[20] Admin. (2024, 11 octobre). *GPS Spoofing Apps Market* -. https://pmarketresearch.com/it/gps-spoofing-apps-market/

[21] Admin. (2024a, février 5). *The Ethical and Legal Quandaries of GPS Data | TrackingFox*. TrackingFox | Car OBD GPS Tracker. https://www.trackingfox.com/2024/01/05/the-ethical-and-legal-quandaries-of-gps-data/

[22] GPS World. (2015, 20 mai). *Going Up Against Time : The Power Grid& # 039 ; s Vulnerability to GPS Spoofing Attacks - GPS World*. https://www.gpsworld.com/wirelessinfrastructuregoing-against-time-13278/

[23] https://www.xmco.fr/actualite-veille-cybersecurite-fr/des-chercheurs-reussissent-a-mettre-en-place-une-attaque-par-usurpation-gps-sur-des-systemes-de-navigation-routiere/

Conséquences sur la Société

Le spoofing GPS peut avoir des conséquences dévastatrices, allant de la désinformation à la perturbation des services essentiels.

Dans le secteur aérien, une attaque par spoofing GPS entraîne des coûts indirect tel que des retards, des déroutements, des fausses alertes et une surcharge de travail pour les équipages.

Selon un rapport détaillé de « OPSGroup », le nombre d'incidents de spoofing a augmenté de 400 % ces dernières années [24].

L'Association internationale du transport aérien (IATA) a rapporté une augmentation de 500 % des incidents de spoofing en 2024 par rapport à l'année précédente.

Les incidents documentés suggèrent que les coûts indirects peuvent être considérables. Une étude britannique a estimé la perte économique due à une coupure du signal GPS de 7 jours à 7,6 milliard d'euros. Les demandes dans les services d'urgence, la mer et la route représentent ensemble 87,6 % de la perte économique totale.

[24] OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024b, septembre 6). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP. https://ops.group/blog/gps-spoofing-final-report/

[25] *The economic impact on the UK of a disruption to GNSS - Executive summary*. (2023b, octobre 18). GOV.UK. https://www.gov.uk/government/publications/report-the-economic-impact-on-the-uk-of-a-disruption-to-gnss/the-economic-impact-on-the-uk-of-a-disruption-to-gnss-executive-summary?

4. Cadre Juridique et Réglementaire

Lois et Régulations

Le spoofing GPS ou usurpation de position GPS est considéré comme une activité illégale dans de nombreux pays en raison de ses implications potentielles sur la sécurité nationale et individuelle. Il est encadré par des lois au niveau national et international.

En France, bien que le Code pénal ne mentionne pas explicitement le spoofing GPS, des infractions connexes peuvent être retenues, notamment l'usurpation d'identité ou l'entrave aux systèmes de communication. L'utilisation de dispositifs de spoofing est généralement interdite, sauf autorisation spécifique.

Usurpation d'identité : Selon l'article 226-4-1 du Code pénal, l'usurpation d'identité, y compris géographique via le spoofing GPS, peut être punie d'une peine d'emprisonnement et d'une amende [26].

Entrave aux systèmes de communication : L'article 323-1 du Code pénal punit l'accès frauduleux à un système de traitement automatisé de données, ce qui peut inclure l'utilisation de spoofing GPS pour perturber des systèmes de navigation [27].

Réglementation des équipements radioélectriques : La Directive européenne 2014/53/UE (RED) interdit la mise sur le marché de dispositifs susceptibles de perturber les réseaux ou d'utiliser de manière abusive les ressources du spectre radioélectrique, ce qui inclut les dispositifs de spoofing GPS [28].

Au niveau international d’autres directives existent en fonction du domaine concerné par le spoofing GPS. la Chine a mis en place des lois strictes pour protéger ses systèmes de navigation par satellite, tandis que l'Union européenne travaille sur des directives pour renforcer la résilience des infrastructures GPS. Ces efforts montrent une reconnaissance mondiale de la menace posée par le spoofing GPS et la nécessité de mesures juridiques pour le contrer.

La Commission Européenne surveille les interférences affectant les systèmes globaux de navigation par satellite européens, tels que Galileo et a initié des activités pour localiser les sources d'interférences [29].

L’Union Internationale des Télécommunications appelle les États membres à prendre des mesures pour éviter la prolifération et l'exploitation de dispositifs non autorisés pouvant interférer avec les systèmes de navigation par satellite, tels que le GPS [30].

L’Organisation de l'Aviation Civile Internationale recommande aux états de surveiller, localiser et stopper les sources d'interférences intentionnelles, y compris le spoofing GPS, afin de garantir la sécurité de l'aviation civile [31].

[26] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593

[27] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/2015-07-27

[28] *Directive - 2014/53 - EN - EUR-LEX*. (s. d.). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014L0053

[29] Cordis, C. (2019, 1 février). *De nouvelles solutions pour éviter les manipulations frauduleuses des systèmes GPS des véhicules*. CORDIS | European Commission. https://cordis.europa.eu/article/id/247410-new-system-prevents-fooling-of-a-vehicles-gps-tracking/fr

[30] Dyer, L., & Dyer, L. (2024, 1 mai). *No more jammer sales : it's time for global enforcement*. SpaceNews. https://spacenews.com/no-more-jammer-sales-its-time-for-global-enforcement/

[31] https://politique.pappers.fr/question/response-to-gps-jamming-and-spoofing-QECR971594

5. Analyse des Risques et Menaces

La falsification des signaux GPS peut également affecter notre compréhension du réel géographique. En manipulant les données de localisation, le spoofing GPS peut créer une dissonance entre la réalité physique et la représentation numérique de l'espace. Cette dissonance peut entraîner une méfiance envers les technologies de navigation et une remise en question de notre dépendance à ces systèmes pour la compréhension de notre environnement.

Les tensions entre l'espace physique et l'espace numérique sont exacerbées par des pratiques comme le spoofing GPS. Ces tensions reflètent les défis de concilier notre expérience tangible du monde avec les représentations numériques qui peuvent être manipulées.

Le spoofing GPS illustre ces tensions entre l'espace physique et numérique en créant des écarts entre ce que nous percevons comme réel et ce qui est représenté numériquement. Cette dissonance peut entraîner des conflits dans la prise de décision, dans la planification urbaine et la gestion des ressources.

Risques pour la Sécurité Nationale

Dans le domaine de l'armée et de la défense, l'usurpation GPS sert à la fois des objectifs offensifs et défensifs. Les forces armées du monde entier reconnaissent le potentiel de cette technologie pour obtenir des avantages tactiques dans les zones de conflit. En manipulant les signaux GPS, les stratèges militaires peuvent créer de fausses impressions de mouvements de troupes, induire en erreur les forces ennemies ou protéger des sites sensibles contre des personnes ciblées. Une application courante est la création de « zones de refus du GPS » autour d'installations militaires critiques. Ces zones utilisent des techniques d'usurpation pour brouiller ou désorienter les armes (bombes ou missiles) guidées par GPS ou les drones de surveillance qui pourraient s'approcher. En outre, les forces militaires peuvent utiliser l'usurpation de GPS pour protéger leur propre personnel et leur matériel en masquant leurs véritables positions pendant les opérations. La technologie joue également un rôle dans les exercices d'entraînement, permettant au personnel militaire de simuler divers scénarios liés au GPS sans avoir besoin d'opérations sur le terrain. Cette application aide à préparer les troupes pour les perturbations GPS potentielles ou les manipulations qu'elles pourraient rencontrer dans des conflits du monde réel [32].

De plus, les infrastructures critiques, telles que les réseaux électriques et les systèmes de transport ou les ports dépendent souvent du GPS pour leur synchronisation et leur fonctionnement [33].

Les systèmes financiers dépendent aussi de la synchronisation précise des horloges, souvent fournie par le GPS. Le spoofing peut entraîner des erreurs de transaction, des fraudes et des perturbations des marchés financiers [34].

Perturbation des télécommunications : Les réseaux cellulaires reposent sur des signaux de synchronisation précis fournis par le GPS. L'usurpation pourrait supprimer cette synchronisation, conduire à des pannes de service, à des appels abandonnés, et potentiellement même à des pannes de communication à grande échelle [35].

Les réseaux électriques modernes, notamment les « smart grids » combinent les technologies du numérique et de l'électricité. Elles sont intégrées au sein des sites de production, dans les infrastructures réseau et jusque chez les consommateurs, afin d'optimiser l'ensemble des mailles du réseau d'électricité. Ceux ci reposent sur une synchronisation temporelle précise fournie par le GPS. Une attaque de spoofing peut induire des erreurs de synchronisation, compromettant la stabilité du réseau et pouvant entraîner des pannes à grande échelle[36].

[32] Caesar, J. (2024b, décembre 16). *What Is GPS Spoofing ? A Look at Its Risks and Solutions*. Tech Review Advisor. https://techreviewadvisor.com/what-is-gps-spoofing/

[33] Krishna. (2024, 25 novembre). *GPS Spoofing : A Silent Threat to High Net-Worth Individuals and Critical Infrastructure*. Krishna Gupta. https://krishnag.ceo/blog/gps-spoofing-a-silent-threat-to-high-net-worth-individuals-and-critical-infrastructure/

[34] Safran, Navigation and Timing. (2024, 30 septembre). *Serveurs de temps en réseau - Safran*. Safran - Navigation & Timing. https://safran-navigation-timing.com/fr/solution/serveurs-de-temps/

[35] *GPS Spoofing : The Hidden Danger to Our Digital World – Techquity India*. (2024, 6 mai). https://www.techquityindia.com/gps-spoofing-the-hidden-danger-to-our-digital-world/

[36] Krishna. (2024b, novembre 25). *GPS Spoofing : A Silent Threat to High Net-Worth Individuals and Critical Infrastructure*. Krishna Gupta. https://krishnag.ceo/blog/gps-spoofing-a-silent-threat-to-high-net-worth-individuals-and-critical-infrastructure/

Mesures de protection

Nos sociétés hyperconnectées doivent faire face à des défis technologiques majeurs pour détecter et prévenir le spoofing GPS. Les avancées technologiques, telles que l'utilisation de l'intelligence artificielle et du machine learning pour la détection des attaques de spoofing, sont cruciales. Des recherches récentes ont montré comment des algorithmes avancés peuvent être utilisés pour identifier et neutraliser les signaux GPS falsifiés. Ces technologies offrent des solutions prometteuses pour améliorer la résilience des systèmes de navigation.

Pour atténuer les risques liés au spoofing GPS, plusieurs mesures peuvent être envisagées :

Authentification des signaux GPS : Développement de protocoles permettant de vérifier l'intégrité des signaux GPS reçus [37].

Redondance des systèmes de navigation : Utilisation de systèmes alternatifs tels que les systèmes de navigation inertielles autonomes pour compléter les données GPS [38].

Détection d'anomalies : Mise en place de systèmes capables d'identifier les incohérences dans les données de positionnement et de synchronisation [39].

Détection de comportements anormaux via l'IA. Les modèles d'IA peuvent analyser les données de localisation pour détecter des anomalies ou incohérences qui pourraient indiquer un spoofing : vitesse ou trajectoires impossibles (ex : un objet se déplace trop vite ou « saute » de position de façon non naturelle). Comparaison avec des données historiques pour repérer les écarts suspects par rapport aux trajets habituels. Réseaux de neurones ou modèles de séries temporelles pour prédire la localisation attendue et signaler les écarts.

Fusion de capteurs, l'IA peut fusionner les données GPS avec d'autres capteurs, tels que : accéléromètres, gyroscopes, Données Wi-Fi, Bluetooth, données de signaux cellulaires, baromètres.

Apprentissage supervisé pour la détection, On peut entraîner un modèle de machine « learning » avec des exemples de trajets valides (non falsifiés), trajets « spoofés » (via simulateurs ou attaques connues). Le modèle apprend à différencier les deux types de données en fonction de leurs caractéristiques statistiques.

Pour les systèmes ayant accès aux signaux brut GPS, l'IA peut détecter des caractéristiques physiques suspectes (ex : puissance du signal, temps d'arrivée incohérents), identifier des signatures de spoofing dans les signaux reçus. Cela nécessite souvent une IA embarquée sur des équipements professionnels ou militaires.

Exemples d'applications concrètes : drones autonomes : vérification croisée des capteurs pour éviter les détournements. véhicules autonomes : détection d'anomalies de navigation en temps réel. Logistique / transport : authentification de la position des camions contre la fraude. Smartphones, détection de triche dans les jeux ou services basés sur la localisation [40] [41] [42] [43].

[37] https://gpspatron.com/wp-content/uploads/2023/11/GPSPATRON-White-Paper-v20.pdf

[38] OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024c, septembre 6). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP. https://ops.group/blog/gps-spoofing-final-report/

[39] Krishna. (2020, 31 mai). *Blog - Krishna Gupta*. Krishna Gupta. https://krishnag.ceo/blog/

[40] Ren, Y., Restivo, R. D., Tan, W., Wang, J., Liu, Y., Jiang, B., Wang, H., & Song, H. (2023b). Knowledge Distillation-Based GPS Spoofing Detection for Small UAV. *Future Internet*, *15*(12), 389. https://doi.org/10.3390/fi15120389

[41] Dasgupta, S., Rahman, M., Islam, M., & Chowdhury, M. (2021, 5 juin). *Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles*. arXiv.org. https://arxiv.org/abs/2106.02982

[42] Ghanbarzade, A., & Soleimani, H. (2025, 4 janvier). *GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning*. arXiv.org. https://arxiv.org/abs/2501.02352

[43] Wang, P., Yang, Z., Li, J., & Shi, L. (2025, 10 janvier). *Learning-based Detection of GPS Spoofing Attack for Quadrotors*. arXiv.org. https://arxiv.org/abs/2501.07597

8. Conclusion

Le spoofing GPS est une technologie complexe avec des implications profondes pour la sécurité, la navigation et la défense. Cette étude a exploré les dimensions techniques, sociales, éthiques et juridiques du spoofing GPS, offrant une perspective holistique sur cette menace et les mesures nécessaires pour la contrer.

Nos sociétés hyperconnectées nous obligent à continuer à étudier et à comprendre les enjeux du spoofing GPS afin de développer des mesures de sécurité efficaces et protéger les infrastructures critiques contre les attaques. Cela passe aussi par les sciences humaines aidées de l'Intelligence Artificielle. L'avenir, c'est maintenant.

9. Références

[1]. http://webriviere.free.fr/sciences/rapports/expose/tempsfreq.pdf

[2]. Letemps1biere. (2025, 23 janvier). Qui étaient les naufrageurs ? - Le temps d& # 039 ; une bière. *Le Temps d'une Bière*. https://letempsdunebiere.ca/ggaspesie-terre-naufrageurs/

[3]. Android MT. (2021, 17 octobre). *Tuto Express : GPS Spoofing, contrôlez la localisation de votre tel Android* [Vidéo]. YouTube. https://www.youtube.com/watch?v=DLOB0nn-kgE

[4]. Gilbert, J., & Gilbert, J. (2024, 31 octobre). *La localisation de précision au service de l'industrie 4.0*. Sysnav | High Precision Positioning For Critical Decisions. https://www.sysnav.fr/localisation-de-precision-au-service-de-lindustrie40/

[5]. OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024, 6 septembre). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP.https://ops.group/blog/gps-spoofing-final-report/

[6] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302450

[7] https://www.areion24.news/2023/10/23/la-securite-des-communications-par-satellite-une-infrastructure-critique-pour-la-transmission-de-donnees

[8] https://www.areion24.news/2023/10/23/la-securite-des-communications-par-satellite-une-infrastructure-critique-pour-la-transmission-de-donnees

[9] https://www.electronicspecifier.com/news/analysis/uk-consumers-are-concerned-about-the-risk-of-gps-spoofing

[10] http://scripties.hzs.be/Repository/Eindwerk_Definitief_2618_1670079390.pdf

[11] https://www.uber.com/es/en/drive/driver-app/fraud- activities/

[12] Guy, A. R. (2024, 15 juin). *Exploring the Ethics of Pokemon Go Location Spoofing*. PrivacyPortal. https://www.privacyportal.co.uk/blogs/free-rooting-tips-and-tricks/exploring- the-ethics-of-pokemon-go-location-spoofing

[13] Caesar, J. (2024, 16 décembre). *What Is GPS Spoofing ? A Look at Its Risks and Solutions*. Tech Review Advisor. https://techreviewadvisor.com/what-is-gps-spoofing/

[14] https://pure.unamur.be/ws/portalfiles/portal/51733550/8627.pdf

[15] Guy, A. R. (2024b, juin 15). *Exploring the Ethics of Pokemon Go Location Spoofing*. PrivacyPortal. https://www.privacyportal.co.uk/blogs/free-rooting-tips-and-tricks/exploring- the-ethics-of-pokemon-go-location-spoofing

[16] *Définition - Placement sous surveillance électronique mobile / PSEM / PSEM | Insee*. (s. d.). https://www.insee.fr/fr/metadonnees/definition/c1833

[17] https://www.leparisien.fr/archives/des-ondes-pour-brouiller-les-pistes-13-05-2015-4766283.ph

[18] *Un yacht piraté en détournant le signal GPS*. (s. d.-b). LeMondeInformatique. https://www.lemondeinformatique.fr/actualites/lire-un-yacht-pirate-en-detournant-le-signal-gps-54563.html

[19] Apte, A., Ingole, V., Lele, P., Marsh, A., Bhattacharjee, T., Hirve, S., Campbell, H., Nair, H., Chan, S., & Juvekar, S. (2019). Ethical considerations in the use of GPS-based movement tracking in health research – lessons from a care-seeking study in rural west India. *Journal Of Global Health*, *9*(1). https://doi.org/10.7189/jogh.09.010323

[20] Admin. (2024, 11 octobre). *GPS Spoofing Apps Market* -. https://pmarketresearch.com/it/gps-spoofing-apps-market/

[21] Admin. (2024a, février 5). *The Ethical and Legal Quandaries of GPS Data | TrackingFox*. TrackingFox | Car OBD GPS Tracker. https://www.trackingfox.com/2024/01/05/the-ethical-and-legal-quandaries-of-gps-data/

[22] GPS World. (2015, 20 mai). *Going Up Against Time : The Power Grid& # 039 ; s Vulnerability to GPS Spoofing Attacks – Gps World*.https://www.gpsworld.com/wirelessinfrastructuregoing-against-time-13278/

[23] https://www.xmco.fr/actualite-veille-cybersecurite-fr/des-chercheurs-reussissent-a- mettre-en-place-une-attaque-par-usurpation-gps-sur-des-systemes-de-navigation-routiere/

[24] OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024b, septembre 6). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP. https://ops.group/blog/gps-spoofing-final-report/

[25] *The economic impact on the UK of a disruption to GNSS - Executive summary.* (2023b, octobre 18). GOV.UK. https://www.gov.uk/government/publications/report-the-economic-impact-on-the-uk-of-a-disruption-to-gnss/the-economic-impact-on-the-uk-of-a-disruption-to-gnss-executive-summary?

[26] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593

[27] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/2015-07-27

[28] *Directive - 2014/53 - EN - EUR-LEX*. (s. d.). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014L0053

[29] Cordis, C. (2019, 1 février). *De nouvelles solutions pour éviter les manipulations frauduleuses des systèmes GPS des véhicules*. CORDIS | European Commission. https://cordis.europa.eu/article/id/247410-new-system-prevents-fooling-of-a-vehicles-gps-tracking/fr

[30] Dyer, L., & Dyer, L. (2024, 1 mai). *No more jammer sales : it's time for global enforcement*. SpaceNews. https://spacenews.com/no-more-jammer-sales-its-time-for-global-enforcement/

[31] https://politique.pappers.fr/question/response-to-gps-jamming-and-spoofing-QECR971594

[32] Caesar, J. (2024b, décembre 16). *What Is GPS Spoofing ? A Look at Its Risks and Solutions*. Tech Review Advisor. https://techreviewadvisor.com/what-is-gps-spoofing/

[33] Krishna. (2024, 25 novembre). *GPS Spoofing : A Silent Threat to High Net-Worth Individuals and Critical Infrastructure*. Krishna Gupta. https://krishnag.ceo/blog/gps-spoofing-a-silent-threat-to-high-net-worth-individuals-and-critical-infrastructure/

[34] Safran, Navigation and Timing. (2024, 30 septembre). *Serveurs de temps en réseau - Safran*. Safran - Navigation & Timing. https://safran-navigation-timing.com/fr/solution/serveurs-de-temps/

[35] *GPS Spoofing : The Hidden Danger to Our Digital World – Techquity India*. (2024, 6 mai). https://www.techquityindia.com/gps-spoofing-the-hidden-danger-to-our-digital-world/

[36] Krishna. (2024b, novembre 25). *GPS Spoofing : A Silent Threat to High Net-Worth Individuals and Critical Infrastructure*. Krishna Gupta. https://krishnag.ceo/blog/gps-spoofing-a-silent-threat-to-high-net-worth-individuals-and-critical-infrastructure/

[37] https://gpspatron.com/wp-content/uploads/2023/11/GPSPATRON-White-Paper-v20.pdf

[38] OPSGROUP Team & OPSGROUP Team 6 September, 2024. (2024c, septembre 6). *GPS Spoofing : Final Report published by WorkGroup*. International Ops 2025 - OPSGROUP. https://ops.group/blog/gps-spoofing-final-report/

[39] Krishna. (2020, 31 mai). *Blog - Krishna Gupta*. Krishna Gupta. https://krishnag.ceo/blog/

[40] Ren, Y., Restivo, R. D., Tan, W., Wang, J., Liu, Y., Jiang, B., Wang, H., & Song, H. (2023b). Knowledge Distillation-Based GPS Spoofing Detection for Small UAV. *Future Internet*, *15*(12), 389. https://doi.org/10.3390/fi15120389

[41] Dasgupta, S., Rahman, M., Islam, M., & Chowdhury, M. (2021, 5 juin). *Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles*. arXiv.org. https://arxiv.org/abs/2106.02982

[42] Ghanbarzade, A., & Soleimani, H. (2025, 4 janvier). *GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning*. arXiv.org. https://arxiv.org/abs/2501.02352

[43] Wang, P., Yang, Z., Li, J., & Shi, L. (2025, 10 janvier). *Learning-based Detection of GPS Spoofing Attack for Quadrotors*. arXiv.org. https://arxiv.org/abs/2501.07597