Détection d'anomalies ADS-B dans le contexte d'aéronefs basse altitude

Melvyn Pirolley, Raphaël Couturier, Michel Salomon, Fabrice Ambert

Détection d'anomalies ADS-B dans le contexte d'aéronefs basse altitude

Melvyn Pirolley[1]
melvyn.pirolley@univ-fcomte.fr

Raphaël Couturier[1]
raphaël.couturier@univ-fcomte.fr

Michel Salomon[1]
michel.salomon@univ-fcomte.fr

Fabrice Ambert[1]
fabrice.ambert@univ-fcomte.fr

[1] IUT Nord Franche-Comté
Institut FEMTO-ST, CNRS, Université de Franche-Comté, Belfort, France

Thèmes – *Informatique*

Résumé – *Depuis quelques années, l'augmentation de la densité du trafic aérien a apporté de nouveaux défis pour les contrôleurs aériens. La surveillance du ciel est devenue plus difficile qu'auparavant et les outils actuels de contrôles aériens ont besoin d'être améliorés. Ce papier présente un algorithme basé sur le Deep-Learning, capable de détecter automatiquement des aéronefs utilisant l'usurpation d'identité dans le but de pouvoir voler, sans attirer l'attention, au dessus de zones sensibles pour y mener une attaque. De plus, avec l'arrivée certaine de services de livraison par drone, le trafic basse altitude est susceptible de fortement se développer dans les années à venir. La diversité de ce trafic risque donc d'être utilisée par des personnes malintentionnées pour y mener des attaques. C'est donc pour cette raison que notre étude se concentre sur le contrôle du trafic à basse altitude. Notre approche utilise un modèle de réseau de neurones qui classifie les trajectoires par type d'aéronefs et met en valeur des anomalies entre la trajectoire et le type d'aéronefs que les appareils prétendent être. L'approche que nous proposons est capable de détecter les attaques d'usurpation d'identité avec une précision de 96,2%.*

Mots-clés – *Cybersécurité, Aviation basse altitude, Machine Learning*

1 Introduction

Depuis quelques années, plusieurs entreprises ont multiplié les essais de systèmes de livraisons automatiques par drones. Nous savons que dans un futur proche, les drones prendront une place importante dans le trafic basse altitude. De plus, ces technologies évoluent en parallèle dans un contexte militaire et les drones pourraient être utilisés de façon malveillante. Nous avons à partir de là, imaginé un scénario d'attaque prenant place dans le contexte de la Coupe du monde de rugby 2023 à Toulouse. Un attaquant pourrait utiliser un drone et cibler le stade tout en usurpant l'identité d'un hélicoptère du SAMU. Le drone émettrait de faux signaux de suivi de vols en ADS-B [1] ou en FLARM [2], pour faire croire aux contrôleurs aériens qu'un hélicoptère du SAMU est en intervention dans la zone. L'une des seules façons de détecter cette attaque serait de relever que la trajectoire du drone est illogique pour être un hélicoptère du SAMU. Notre projet est dans la continuité de ces deux travaux [1, 2].

2 Jeu de données

Avec l'objectif d'avoir un jeu de données important et Open Source, la base de données de la communauté OpenSky Network a été utilisée. Elle contient un historique de messages ADS-B émis par des aéronefs partout dans le monde depuis plus de 7 ans. Pour notre scénario, nous nous sommes restreint aux messages ayant été reçus autour de Toulouse dans une zone qui va de Saint-Gaudens à Carmaux. Les coordonnées précises de cette zone partent de lat. 0.72561, lon. 43.11581 à lat. 2.16344, lon. 44.07449. Afin de conserver uniquement le trafic basse altitude, seulement les messages sous 10000 pieds sont conservés. Notre jeu de données est composé de traces récentes, sur l'année 2022 complète. Après filtrage, notre jeu de données est constitué de 10 158 vols pour l'entraînement et 819 pour l'évaluation. Les trajectoires sont enregistrées dans des fichiers CSV, incluant les champs classiques des messages ADS-B et FLARM tels que la latitude, la longitude, l'altitude, la vitesse, l'orientation... Pour finir, les données sont labellisées en associant le code d'immatriculation de chaque appareil à un type parmi : **avion de ligne** au décollage ou à l'atterrissage, **avion de tourisme** pour des avions légers comportant entre 2 et 6 sièges, et enfin les **hélicoptères** du SAMU.

3 Méthode

Pour détecter les attaques d'usurpation d'identité, nous avons développé un réseau de neurones profond à convolutions (Convolutional Neural Network) qui détermine le type des aéronefs à partir de leurs trajectoires. Un modèle correctement entraîné sera alors capable d'identifier les usurpations d'identité en montrant une anomalie entre le type prétendu de l'appareil et sa trajectoire. Nous avons aussi essayé d'utiliser les réseaux Long-Short Term Memory, spécifiquement câblés pour les séries temporelles, et les Transformers qui intègrent un mécanisme appelé l'attention permettant de pondérer positivement les portions intéressantes de la série temporelle. Malgré le fait que les CNN soient normalement adaptés au traitement d'images, ils nous donnent de meilleures performances. Afin de traiter des trajectoires de longueurs variables, notre modèle utilise une fenêtre glissante avec un historique fixe de 128 pas de temps (environ deux minutes de vol). À la fin, on obtient pour chaque message ADS-B, une prédiction du modèle. Pour obtenir la prédiction finale, l'algorithme conserve seulement la prédiction avec la confiance la plus élevée. En temps normal, utiliser un système de vote par majorité pourrait paraître plus logique, mais dans notre situation, il mène à des performances inférieures car les motifs réellement importants ne sont pas forcément majoritaires. Typiquement, à altitude de croisière, les trajectoires sont longues et régulières, dépourvues de motifs permettant d'en déduire le type de l'appareil avec précision.

3.1 Contexte de décollage

Pour améliorer les capacités de détection, nous avons ajouté, en entrée secondaire, un contexte de décollage. Il contient les 128 premiers pas de temps de la trajectoire incluant donc la « forme » du décollage de l'appareil. Le décollage est très important car il contient des informations cruciales sur le type de l'appareil. Par exemple, seulement les hélicoptères possèdent la capacité de décoller verticalement.

3.2 Contexte géographique

De même, nous avons eu l'idée d'ajouter un contexte géographique en entrée du réseau de neurones car les trajectoires des aéronefs dépendent de leur environnement. Par exemple, les hélicoptères du SAMU suivent la Garonne au décollage pour des raisons de nuisances sonores. Ce contexte est une image de carte OpenStreetMap centrée sur la position de l'appareil comme l'illustre la Figure 1. Cette donnée apporte au modèle des informations géographiques supplémentaires, comme la position des rivières, des forêts et des zones urbaines qui entourent l'aéronef. Dans la pratique le modèle extraira de cette images des informations abstraite pour un humain, mais importantes pour déterminer le type de l'aéronef.

De plus, l'utilisation du contexte géographique permet de localiser l'appareil. On peut ainsi utiliser un système de coordonnées relatives permettant au modèle d'apprendre plus facilement. L'espace de nombre nécessaire pour représenter une trajectoire en coordonnées relatives est réduit à

1. Automatic dependent surveillance-broadcast
2. Le FLARM est un protocole similaire à l'ADS-B, très répandu dans le trafic basse altitude, inventé pour éviter les collisions entre aéronefs

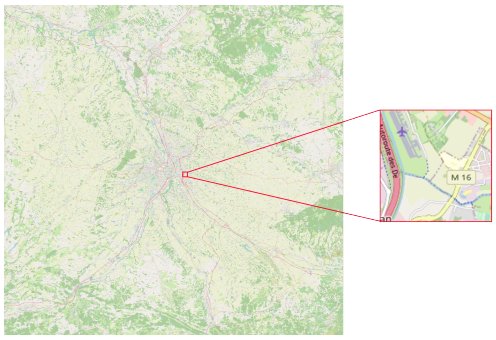

FIGURE 1 – Extraction du contexte géographique à partir de la position de l'aéronef

un rectangle de 50km de diagonale par rapport à un système de coordonnées absolues qui nécessite un rectangle de 155 km de diagonale. Pour générer notre contexte géographique, nous utilisons une image de haute résolution couvrant intégralement notre zone d'étude autour de Toulouse, puis pour chaque aéronef nous prélevons un carré de 128×128 pixels centré sur sa position.

3.3 Architecture du modèle

L'architecture du modèle (Figure 2) est composé de trois couches d'entrée : l'une pour les 128 derniers messages ADS-B et les deux autres pour les vecteurs de contextes qui ont été expliqués précédemment. Les messages ADS-B et le contexte de décollage sont traités par le même réseau de neurones à convolutions à une dimension. Le contexte géographie est traité par un réseau de neurones à convolutions à deux dimensions. Les sorties de ces deux sous-modèles sont ensuite aplaties et concaténées pour être analysées par un réseau de neurones complètement connecté. La couche de sortie est constituée de trois neurones, un pour chaque classe d'appareil présent dans notre étude.

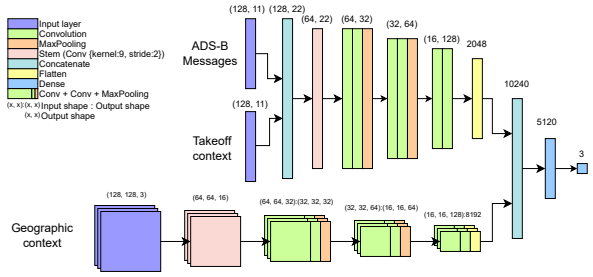

FIGURE 2 – Architecture du modèle

4 Résultats

Afin de vérifier l'efficacité de chaque fraction de notre approche, nous avons évalué plusieurs modèles en partant du plus simple jusqu'à notre modèle complet. La Table 1 montre les résultats de cette étude obtenus sur le jeu de données d'évaluation.

Les résultats montrent que chaque composant de notre modèle améliore légèrement les performances globales.

TABLE 1 – Étude de modèles ablatés

Modèle	**Précision**	**Changement**
CNN Simple	91,2%	
Ajout du décollage	93,5%	+2,3%
Ajout de la géographie	95,1%	+1,6%
Ajout des coordonnées relatives	96,2%	+1,1%

L'ajout du contexte de décollage provoque la plus forte amélioration avec une augmentation de 2,3% des performances. Ensuite l'utilisation de coordonnées relatives améliore de 1,1% les résultats. Cependant, l'utilisation des coordonnées relatives va de pair avec le contexte géographique. La position absolue de l'appareil reste une information cruciale car certaines zones ont des réglementations bien spécifiques. Donc la position absolue de l'appareil doit quand même être fournie au modèle, que ce soit directement via des coordonnées GPS ou alors par le contexte géographique. C'est d'ailleurs pour cette raison que le contexte de décollage est fourni au modèle en position absolue, afin que le modèle puisse savoir précisément depuis quel aéroport l'aéronef a décollé.

5 Conclusion

Ce papier propose une nouvelle architecture de réseaux de neurones profonds conçu spécifiquement pour la détection d'attaques d'usurpation d'identité, sur des messages ADS-B et dans le contexte du trafic aérien basse altitude. Nos résultats sont encourageants avec une précision de 96,2% et nos expériences nous permettent d'affirmer que les réseaux de neurones profonds sont capables de détecter des attaques d'usurpation d'identité.

Cependant, à cause du manque de données, notre modèle actuel n'est pas encore capable de détecter directement les drones. Dans nos prochaines expérimentations, nous allons confronter notre modèle à des trajectoires de drones simulées, très réalistes, fournies par l'ONERA. Nous évaluerons alors les limites du modèle avec des trajectoires de drones volant dans la même zone que les hélicoptères du SAMU.

Références

[1] Ralph Karam, Michel Salomon, and Raphaël Couturier. A comparative study of deep learning architectures for detection of anomalous ads-b messages. In *2020 7th International Conference on Control, Decision and Information Technologies (CoDIT)*, volume 1, pages 241–246. IEEE, 2020.

[2] Antoine Chevrot, Alexandre Vernotte, and Bruno Legeard. Cae : Contextual auto-encoder for multivariate time-series anomaly detection in air transportation. *Computers & Security*, 116 :102652, 2022.