MENACE SUR LE TRAFIC AÉRIEN

Par Paul-Emmanuel Vandenburie, Ingénieur chez Airbus CyberSecurity, Diplômé du MS Cybersécurité de l'ISEP*

Issu d'un travail de recherche dans le cadre d'une thèse sur la « Sécurité dans l'avionique », cet article présente les risques et les solutions actuellement identifiées d'un système particulier : l'ADS-B. Il montre ainsi comment les choix industriels résultent de l'analyse de coûts et de l'évolution possible des protocoles.

LE SYSTÈME DE GÉOLOCALISATION PAR ADS-B

Le système ADS-B (Automatic Dependant Surveillance – Broadcast), équipant maintenant la quasi-totalité des avions, permet à un appareil d'envoyer sa position par radio, ainsi que d'autres informations telles que son identification, sa vitesse ou son cap : c'est « l'ADS-B OUT ».

Les stations au sol, les tours de contrôle, et parfois les autres avions, disposent d'un récepteur « ADS-B IN » afin d'écouter les messages des avions environnants, et ainsi connaître leur position en temps réel.

Il faut savoir que la surveillance par radar actuelle est coûteuse à maintenir et possède une couverture limitée. Proposé par la FAA (American Federal Aviation Administration), **NextGen** est le nouveau framework de surveillance aérienne visant à remplacer la surveillance traditionnelle par radars et l'ADS-B en est un composant essentiel.

Figure 1: Suivi d'un vol en temps réel (FlightAware.com)

Toutefois, lorsque le système ADS-B a été conçu, la sécurité n'était pas la priorité, et il ne dispose donc d'aucun mécanisme permettant l'authentification de l'émetteur ou le chiffrement des messages. Or aujourd'hui, la conception d'un récepteur est à la portée de toutes les bourses.

Ainsi, la nature ouverte de l'ADS-B et le faible prix des récepteurs a permis l'apparition de sites de suivi des vols en temps réel (ou « flight tracking »), tels que **FlightAware**. Ceux-ci nouent des partenariats avec les professionnels ou les particuliers passionnés disposant d'un récepteur ADS-B afin d'obtenir la plus grande couverture possible. Pour pallier les nombreuses zones blanches, ces sites proposent à leurs visiteurs particuliers d'acheter un récepteur, cette solution étant aujourd'hui bon marché, voire fournissent un tutoriel afin de construire son propre récepteur « low-cost ».

CONSTRUIRE UN RÉCEPTEUR LOW-COST

Il existe de nombreux sites et vidéos décrivant pas à pas la confection d'une station de réception ADS-B à destination des particuliers, s'attachant à fournir une solution facile à utiliser et abordable financièrement. On y trouve également des tests comparatifs de récepteurs radio, ainsi que des conseils d'installation pour obtenir la meilleure réception possible. En bref, une station d'écoute low-cost consiste en l'assemblage des composants suivants :

- **L'ordinateur :** n'importe quel ordinateur peut être utilisé pour traiter le signal reçu. Or la possibilité de recevoir les signaux ADS-B et de les partager sur Internet 24h/24 implique de s'intéresser à la consommation électrique. Un ordinateur portable consommant autour de 60 Watts, il est conseillé d'utiliser plutôt un ordinateur « de poche », généralement un Raspberry Pi, la version 3 ne consommant qu'environ 2 Watts, et se trouve à moins de 70€.

TECHNICAL REVIEW

Threats to air traffic

*By Paul-Emmanuel Vandenburie, Engineer at Airbus CyberSecurity, Graduate of MS Cybersecurity, ISEP **

Based on research work on a thesis on "Security in avionics", this article covers the risks and solutions currently identified for a particular system: ADS-B. It demonstrates how industrial choices result from cost analysis and the likely development of protocols.

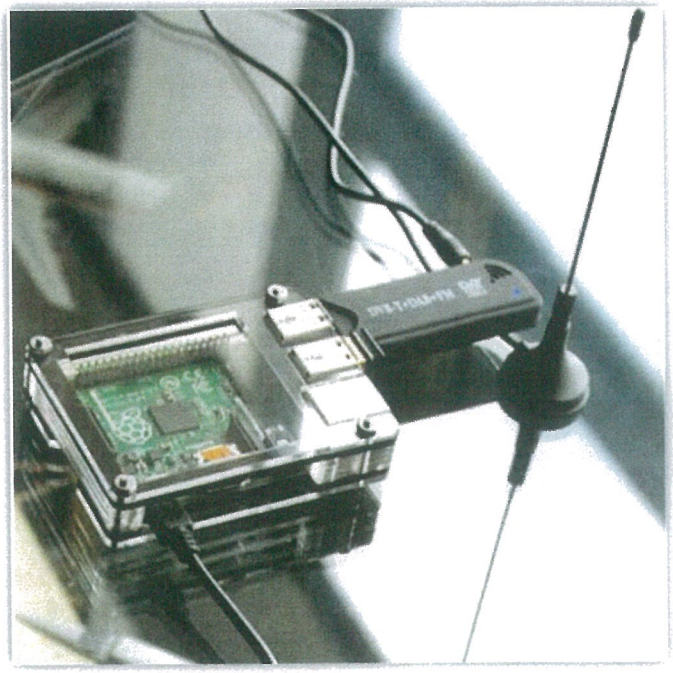

Figure 2: Récepteur ADS-B (RaspberryPi et dongle radio)

- **Le logiciel de traitement :** le cas le plus répandu étant l'utilisation d'un Raspberry, FlightAware fournit gratuitement une image logicielle « PiAware » à télécharger et installer sur la carte SD du Raspberry. La connexion Internet peut se faire via l'interface Ethernet ou Wi-Fi, et permettra de partager les données avec le site FlightAware.

- **Le récepteur radio :** alors qu'un récepteur radio coûtait plusieurs centaines, voire milliers d'euros il y a quelques années, les radios logicielles (**SDR – Software Defined Radio**) modernes permettent aujourd'hui de recevoir n'importe quel type de signal par simple reconfiguration logicielle, et ce pour quelques dizaines d'euros. Celles-ci sont fournies avec une connexion USB et s'interfacent facilement avec le Raspberry. Il est ensuite possible d'ajouter un module d'amplification du signal, voire un module de filtrage pour améliorer le signal reçu.

LES MESSAGES ADS-B

Le principe de l'ADS-B est que chaque avion récupère sa propre position et vélocité grâce au GPS embarqué. Ces informations sont alors diffusées via ADS-B OUT aux stations au sol, ainsi qu'aux avions à proximité (s'ils disposent de l'ADS-B IN). D'autres champs sont prévus : notamment un ID identifiant l'avion, ou le plan de vol. Envoyés sur la fréquence 1090 MHz, les messages de 112 bits sont très sensibles aux réflexions de signal et à la dispersion (multi-path).

LES MENACES SUR L'ADS-B

Du fait de sa nature de diffusion radio, l'ADS-B est vulnérable aux attaques suivantes :

- Les messages étant envoyés en clair, il est évidemment très simple d'effectuer **une écoute passive (Eavesdropping)**.

- Commun à toute transmission radio, le **brouillage (Jamming)** peut être effectué très simplement en envoyant un signal sur la fréquence 1090 MHz suffisamment puissant pour que les stations aux alentours ne puissent plus recevoir le message.
  Cependant, lorsque le nombre de stations au sol est élevé, il devient compliqué de brouiller sur une surface étendue. Le risque se pose plutôt aux abords d'un aéroport où le brouillage rend possible un **Déni de service (DoS)** sur les stations au sol (Ground Station Flood Denial), ainsi que sur les avions en vol (Aircraft Flood Denial).

- L'ADS-B n'incluant pas d'authentification des messages, il est très simple **d'injecter des messages** illégitimes correctement formatés, ceci avec des moyens restreints et quelques connaissances du protocole. Une attaque possible est donc l'injection de « faux avions » vers les stations au sol (Ground Stations Target Ghost Injection/Flooding) ou les avions en vol (Aircraft Target Ghost Injection/Flooding).

- Plus subtil que le simple brouillage, la **suppression de message** par l'envoi d'interférences destructrices consiste à effacer ou atténuer suffisamment le message ADS-B en envoyant un signal exactement inverse. Cette technique reste cependant complexe techniquement à mener. L'attaque correspondante étant la disparition d'avion (Aircraft Disappearance).

- Plus complexe que la suppression puis injection de message, la **modification à la volée d'un message légitime** est possible en remplaçant une partie du message en surimposant un nouveau message. Cela rend possible la modification de la trajectoire annoncée (Virtual Trajectory Modification), avec pour conséquence d'augmenter le risque de collision avec un autre avion.

Malgré cela, la nature ouverte de l'ADS-B est considérée comme souhaitable dans de nombreux scénarios, et fait partie intégrante de la manière dont le contrôle du trafic aérien est actuellement géré. Alors même que cette faiblesse est le point de départ d'attaques plus complexes et problématiques.
Ainsi, une démonstration d'attaque a été réalisée par **Hugo Teso** lors de la conférence « Hack in the Box » de 2013 à Amsterdam. Celle-ci a été menée sur un système avionique en laboratoire, mais réputé proche de celui réellement embarqué. Sans être le principal vecteur de l'attaque qui visait l'ordinateur de bord de l'avion (FMS – Flight Management System), l'ADS-B y joue un rôle primordial en permettant la localisation de l'avion ciblé.

Il y reste donc deux principales approches pour la sécurisation de l'ADS-B :

- L'authentification des messages émis visant à garantir l'authenticité de l'émetteur ;

- La vérification de la localisation, permettant de confirmer l'information de position reçue.

COMPLEXITÉ DE MISE EN PLACE DE L'AUTHENTIFICATION

L'authentification des messages est plus compliquée sur une communication broadcastée qu'en point à point. De plus, celle-ci requiert l'utilisation d'un **chiffrement par clés publiques** et la mise en place d'une PKI. Des études ont validé son application à l'ADS-B, mais le concept, connu sous le nom « d'ADS-S » (Automatic Dependent Surveillance System Secure) requiert qu'une base mondiale de clés sécurisées soit maintenue, avec les coûts et risques de failles de sécurité que cela implique. De plus, le système n'est pas compatible avec l'ADS-B actuel.
Une alternative à la complexité de mise en place d'une PKI est de publier rétroactivement les clés d'authentification. Lors de la diffusion de chaque message, un code d'authentification (MAC - Message Authentication Code) est ajouté. Au bout d'un certain temps, la clé de déchiffrement de ce code est publiée. Les récepteurs, qui ont gardé en mémoire les messages précédents, peuvent alors déchiffrer les codes et vérifier l'authenticité de l'émetteur sur tous les messages. Cette technique a été formalisée par le protocole **TESLA** (Time Efficient Stream Loss-Tolerant Authentication) décrit dans la RFC 4082, et **µTESLA** pour son adaptation aux réseaux sans fil. Ce protocole permettant l'authentification à grande échelle de messages diffusés, et supportant la perte de paquets et les contraintes temps réel, pourrait être applicable à l'ADS-B.

VÉRIFICATION SÉCURISÉE DE LA LOCALISATION

Une alternative à l'authentification des communications est de vérifier **l'authenticité de la localisation** diffusée par l'avion. Il ne s'agit plus de vérifier l'intégrité du message et de son émetteur mais bien sa localisation, grâce à la participation de plusieurs récepteurs. Ceux-ci fournissent également une redondance en cas de panne du système de navigation ou du GPS.
La **multilatération**, ou localisation hyperbolique, est un mode de surveillance utilisé dans le monde militaire et civil depuis des décennies. Il consiste à établir la distance précise entre au moins 4 récepteurs, dont la localisation est connue, et un émetteur dont la localisation est inconnue, pour calculer la position de ce dernier.
Il est possible d'appliquer la multilatération au signal ADS-B, en calculant la différence entre les temps de réception (TDOA - Time Difference Of Arrival) sur différentes antennes implantées à des positions différentes pour déterminer la position en 3D de l'avion.
Cette solution présente l'avantage d'utiliser les communications avioniques existantes, sans modification des équipements déjà déployés dans les avions. En revanche, elle nécessite le déploiement au sol d'une infrastructure permettant la réception du signal et le calcul de la position.

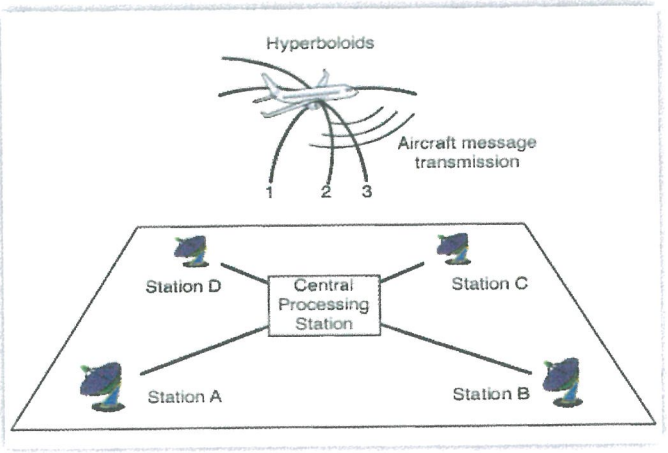

Figure 3: Géolocalisation par multilatération

Cette technique est utilisée notamment pour les courtes distances autour des aéroports : le système ASDE-X pour les aéroports américains, ou le projet CASCADE en Europe.

CONCLUSION

Concernant la protection de l'ADS-B, aucune méthode n'est exempte de défaut ou d'impact sur le déploiement actuel. La question du coût d'une solution s'impose aussi, car elle pèse directement sur les choix industriels. Il s'agit donc de choisir entre un changement complet de protocole, qui adresserait les questions de sécurité de manière plus complète, ou bien un système parallèle requérant du matériel et du logiciel additionnels.
En avionique, le développement d'une solution technique nouvelle, telle que l'ADS-B, sa certification et son déploiement à grande échelle peut prendre parfois plusieurs dizaines d'années. Il n'est donc pas urgent de proposer une révision complète du système de contrôle aérien. Cependant, il est d'ores et déjà important de commencer à étudier les lacunes de l'ADS-B, afin de travailler sur un protocole qui lui succèdera à terme. Et qui, dès sa conception, prendra en compte l'authentification, ainsi qu'une solution pour la gestion des clés de chiffrement. ■■■

* Paul-Emmanuel Vandenburie est Ingénieur chez Airbus CyberSecurity, et Diplômé du MS Cybersécurité de l'ISEP.
Le 31 janvier 2019, à l'occasion de la Remise des diplômes Mastères spécialisés ® « Architecture Cybersécurité et Intégration » de l'école du numérique l'ISEP, Paul-Emmanuel Vandenburie a présenté sa thèse professionnelle sur la « Sécurité dans l'avionique » qui clôt son cycle de formation continue.

Références

PiAware – Construisez votre station ADS-B : https://fr.flightaware.com/adsb/piaware/build

Un Raspberry Pi pour suivre les avions sur FlightRadar24 : https://www.framboise314.fr/un-raspberry-pi-pour-suivre-les-avions-sur-flightradar24-2/#La_solution_d8217Erik

Hack In The Box Security Conference (2013) - Hugo Teso – Aircraft Hacking :
- https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf
- https://www.youtube.com/watch?v=wk1jIKQvMx8

On the Security of the Automatic Dependent Surveillance-Broadcast Protocol : https://www.researchgate.net/publication/305720556_On_the_Security_of_the_Automatic_Dependent_Surveillance-Broadcast_Protocol

RFC4082 Timed Efficient Stream Loss-Tolerant Authentication (TESLA) : https://tools.ietf.org/pdf/rfc4082.pdf