Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department
EURECOM
Sophia-Antipolis, France
Email: andrei.costin@eurecom.fr, aurelien.francillon@eurecom.fr

***Abstract*—In this paper we investigate (in)security aspects of Automatic Dependent Surveillance-Broadcast (ADS-B) protocol. ADS-B is intended to be widely deployed in Air Traffic Management (ATM) Surveillance systems by 2020. One of the goals of ADS-B is to increase safety of air traffic. While the security of ADS-B was previously questioned, in this paper we demonstrate that attacks are both easy and practically feasible, for a moderately sophisticated attacker. Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying of injection).**

The attacks have been implemented using an Universal Software Radio Peripheral (USRP), a widely available Software-Defined Radio (SDR). for which we developed an ADS-B receiver/transmitter chain with GNURadio. We then present and analyze the results of the implemented attacks tested against both USRP-based and commercial-off-the-self (COTS) radio-enthusiast receivers. Subsequently, we discuss the risks associated with the described attacks and their implication on safety of air-traffic, as well as possible solutions on short and long terms. Finally, we argue that ADS-B, which is planned for long-term use, lacks the minimal and necessary security mechanism to ensure necessary security of the air traffic.

***Keywords*-Architecture and Design Air Traffic Control, Air Traffic Management, Automatic Dependent Surveillance-Broadcast, ADS-B, message injection, message replay, wireless security, privacy.**

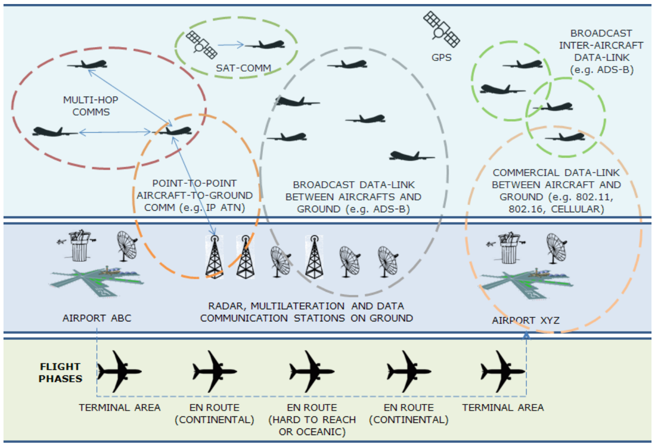
SAT-COMM
GPS
BROADCAST INTER-AIRCRAFT DATA-LINK (e.g. ADS-B)
MULTI-HOP COMMS
POINT-TO-POINT AIRCRAFT-TO-GROUND COMM (e.g. IP ATN)
BROADCAST DATA-LINK BETWEEN AIRCRAFTS AND GROUND (e.g. ADS-B)
COMMERCIAL DATA-LINK BETWEEN AIRCRAFT AND GROUND (e.g. 802.11, 802.16, CELLULAR)
AIRPORT ABC
RADAR, MULTILATERATION AND DATA COMMUNICATION STATIONS ON GROUND
AIRPORT XYZ
FLIGHT PHASES
TERMINAL AREA
EN ROUTE (CONTINENTAL)
EN ROUTE (HARD TO REACH OR OCEANIC)
EN ROUTE (CONTINENTAL)
TERMINAL AREA

Figure 1. Envisioned NextGen airspace system with ADS-B and e-enabled aircrafts according to [4].

I. Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) is an Air Traffic Management and Control (ATM/ATC) Surveillance system that is intended to replace traditional radar based systems and is expected to become an essential part of the Next Generation Air Transportation System (NextGen)-like systems. Figure 1 shows an envisioned by [4], and already partially deployed, architecture for the NextGen-like systems, along with ADS-B as part of it.

The concept behind ADS-B is quite simple and can be summarized as follows: ADS-B avionics broadcast a plain text, unencrypted, error-code protected messages over radio transmission links, approximately once per second. Those messages contain the aircraft's position, velocity, identification, and other ATC/ATM-related information.

For the spatial position derivation, ADS-B is designed to use mainly GPS, though GPS is prone to GPS-derived attacks [53], [54]. However, these GPS-oriented attacks are out of scope of this paper, Tippenhauer et al. provides more details on GPS spoofing in [32]. On the other hand, GPS sensors used in ADS-B devices must comply with ADS-B requirements, specifically with RTCA/DO-229C TSO-C145a [24] (e.g. Garmin GDL 90 [59], Freeflight 120x [60] and others). Those standards specify the requirements for integrity checks on GPS signals, hence allowing ADS-B to withstand most GPS-related attacks. On top, [33] suggests inclusion of spatial accuracy parameters in ADS-B messages to enable GPS error computation by the receiver, while [34] proposes the use of Ground-Based Augmentation System (GBAS) to add resilience to unintentional or intentional GPS errors.

ADS-B can be used for several purposes and has the following intended benefits :

- increased safety of the air-traffic management and control. It is intended to dramatically improve situational awareness of pilots, by providing them access to the same kind of real-time air-traffic information as ATC controllers. For example, will receive information from other aircrafts and information about weather and terrain.

- improve air-traffic conflict detection and resolution. ADS-B will allow planes to know their relative positions, without relying on an infrastructure.
- optimize and compact the air-traffic. The traditional passive radar system has relatively low resolution. Moreover, with traditional radars, accuracy of the position depends on the distance to the plane. Finally, radars usually are not able to provide altitude information. ADS-B has much better coordinates resolution and effective range of 100-200 nautical miles [18] [1]. Therefore, it is expected that ADS-B will allow for a much better use of airspace by allowing to reduce distance between planes, especially near busy airports.

Surprisingly, despite years of standardization ([19] [20] [21] [22] [23]), development, thorough testing, and an ongoing deployment, by design ADS-B protocol used in commercial air-traffic doesn't specify mechanisms to ensure that protocol messages are authentic, non-replayed or adhere to other security properties.

In this paper, our main focus is to demonstrate the easiness, feasibility and practicality, compared to previous works which covered the theoretical aspects of insecurity in ADS-B. For this purpose we set up a practical, low-cost and moderately sophisticated attack against new-generation, high-cost and safety-critical ADS-B technology. Specifically, despite the fact that manual validation procedures exist [25] to partially mitigate the presented attacks, conducting such attacks in continuous and/or distributed fashion on the ATCs and aircrafts greatly increases the chances of human error. For example, under conditions of erroneous or uncertain data, the stress factor, associated with continuous erroneous messages on display of ATC and critical time response requirements, increases and affects the safety of the entire system.

While completely unrelated to ADS-B, it was reported that the effect of erroneous data from wind speed sensors combined with stress factors have played an important role in Air France Flight 447 fatal crash[57]. This combination have practically nullified pilots' basic flight knowledge and well-known recovery procedures, as the final report on the crash attests [58]:

> A crew can be faced with an unexpected situation leading to a momentary but profound loss of comprehension. If, in this case, the supposed capacity for initial mastery and then diagnosis is lost, the safety model is then in "common failure mode". During this event, the initial inability to master the flight path also made it impossible to understand the situation and to access the planned solution.

The question that follows is: would malicious ADS-B messages be sufficient to confuse pilots, or air traffic control personnel, and lead to dangerous maneuvers?

Organization

The rest of this paper is organized as follows: in Section II background and basic details of ADS-B are introduced; then, in Section III we present the main security problems and security models associated with ADS-B. Subsequently, in Section IV we present our setup and used methodology to practically demonstrate problems from Section III; Section V discusses prior work, along with our new findings, prospects for future research and covers existing proposed solutions as well as presents potential solutions and mitigations resulted from our research; finally, Section VI concludes the paper.

II. Background

A. SSR, Transponders and Transponder Modes

Before introducing ADS-B, we define some additional terms and technologies to provide a better understanding of the field. Primary Surveillance Radars (PSR) are radars that detect presence of planes via the reflection of radio waves by the planes. Currently, one of the main ways to keep track of aircrafts and flights is by means of Secondary Surveillance Radars (SSR). A SSR detects and measures the position of aircrafts, as well as requests additional information from the aircrafts. SSR does so by relying on radar transponders installed on aircrafts. Transponders (*trans*mitter-res*ponders*), receive requests and transmit replies in so called interrogation modes. Initially, for civilian/commercial traffic there was Mode-A and Mode-C, whereas Mode-S is an enhanced mode which provides multiple information formats to a *selective* (hence S) interrogation. Every aircraft is assigned a fixed 24-bit ICAO address.

In this context, technology-wise ADS-B is an upgrade to SSR, which is expected to be faded-out and give place to ADS-B as main technology, whereas data-wise ADS-B is an extension of Mode-S.

B. ADS-B Overview

At the physical medium level, ADS-B operates at two radio frequencies: 1030 MHz for the active interrogation, for example from ATC towers, radars or other aircrafts, and 1090 MHz for the active response or normal broadcasts, for example from aircrafts or less commonly from airport vehicles. For interoperability, regulatory and legacy purposes, ADS-B is being supported by two different data links, specifically 1090 MHz Extended Squitter (1090ES) and Universal Access Transceiver (UAT). As part of NextGen ATM systems, ADS-B is being co-developed and co-deployed with Flight Information Services-Broadcast (FIS-B) and Traffic Information Service-Broadcast (TIS-B). Both FIS-B and TIS-B may be susceptible to similar attacks as those described in this paper. However, such protocols are used for less critical information, we therefore did not investigate actual attacks feasibility, which we leave for future work.

[1] Approximately 180-370 km.

In terms of active response and normal broadcasts, the roles of an entity in the ADS-B architecture can be either broadcast transmitter, referred to as ADS-B OUT, or broadcast receiver, referred to as ADS-B IN. Currently, most aircrafts are designated broadcast transmitters and equipped with ADS-B OUT technology. Therefore, theit role in ADS-B is to broadcast their position for further analysis and aggregation at ATC towers and ATM stations.

However, since one of the most advertised benefits of ADS-B is the aircraft pilot's ability to have superior situational awareness, ADS-B IN technology, which is currently deployed mainly in ATC towers, is being deployed and undergoes testing in aircrafts. According to [55], SWISS is pioneering use of ADS-B IN in Europe and is one of only five airlines around the world to participate in the airborne traffic situational awareness (ATSAW) project. ADS-B IN is supposed to enable ATSAW, spacing, separation and self-separation applications. However, from a security point of view, ADS-B IN in aircrafts raises a new set of challenges. For example, reliably verifying online [2] and in real-time the validity of identity, position and flight-paths from a received broadcast. While this scenario is manageable in a ground ATC station, where high-speed connectivity is not an issue, it is more difficult to perform in an aircraft.

At the data-link level, the ADS-B protocol is encapsulated in Mode-S frames. As such, ADS-B uses pulse-position-modulation (PPM) and the replies/broadcasts are encoded by a certain number of pulses, each pulse being 1μs long. Therefore, ADS-B has a data rate of 1 Mbit/sec. The reply/broadcast frames consist of a preamble and a data-block. The preamble, of 8μs long, is used to synchronize the transmitters and receivers, it consists of four pulses with a length of 0.5μs per pulse, with interspaces (to the first pulse) of 1, 3.5 and 4.5μs respectively. It is unspecified whether collision detection (CD) or collision avoidance (CA) on the medium-access level exists for the ADS-B protocol. Data-blocks are either 56 bit or 112 bit long and are used to encode various downlink format (DF) messages. For the purpose of this paper, the most interesting DFs are DF11 (Mode S Only All-Call Reply) and DF17 (1090 Extended Squitter). The secure Mode-S/ADS-B mode, used in military, is encoded in DF19 (Military Extended Squitter), lightly covered by [27], in DF22 (Military use only), covered by [28], [29], [30], [31], and in Mode-5 crypto/secure mode, which uses enhanced cryptography based on time-of-day information and direct sequence spread spectrum modulation as specified in NATO STANAG 4193 and ICAO Annex 10. To the best of our knowledge the exact specifications of DF19, DF22, Mode-5 crypto/secure-more are not public as of time of writing.Figure 2 shows an example ADS-B message with the PPM modulation of an ADS-B encoded short frame (56 bits).

On the non technical side though, upgrade to ADS-B technology assumes massive investments in both time and money. According to [17], FAA (USA) alone estimates that the implementation will occur during the period 2006-2035. In financial terms, the projected total spending for the moment exceeds \$1176M and is expected to be a multi-billion total expenditure by the final implementation and deployment. Despite missing public data from EURECONTROL (EU) and CASA (Australia) related to ADS-B implementation costs, we would assume the investments in time and money to be similar.

Given the budget involved, and the sensitivity of air-traffic, it is surprising that such a system was not desiged with security in mind.

III. Problem formulation

Since ADS-B is supposed to support mission-critical automatic and human decisions, and have direct impact on the overall air-traffic safety, it is imperative that technology behind ADS-B meets operational, performance and security requirements.

However, the main problem with ADS-B is the lack security mechanisms, specifically:

- lack of entity authentication to protect against message injection from unauthorized entities.
- lack of message signatures or authentication codes to protect against tampering of messages or impersonating aircrafts.
- lack of message encryption to protect against eavesdropping.
- lack of challenge-response mechanisms to protect against replay attacks.
- lack of ephemeral identifiers to protect against privacy tracking attacks.

We did not include Denial of service (DoS), e.g., by jamming radio signals, because it affects RF-based communication in general, and is not specific to ADS-B.

A. Attacker Model

Building a correct adversary model is essential in assessing the potential of their actions on the a system. In the ADS-B system, an attacker can be classified using several properties like his/her place in the system, physical position and his goals.

1) Place in The System:

- *external* - An external attacker has a higher probability of existence. Since it is external to the system he/she doesn't require authentication or authorization and can execute low-cost attacks easily and can virtually belong to any group of the Classification III-A3;
- *internal/insider* - This is a person trusted by the system. For example he/she can be a pilot, an ATC controller, an airport technician, etc. This type of attacker has a lower

[2] To check different data sources such as flights plans.

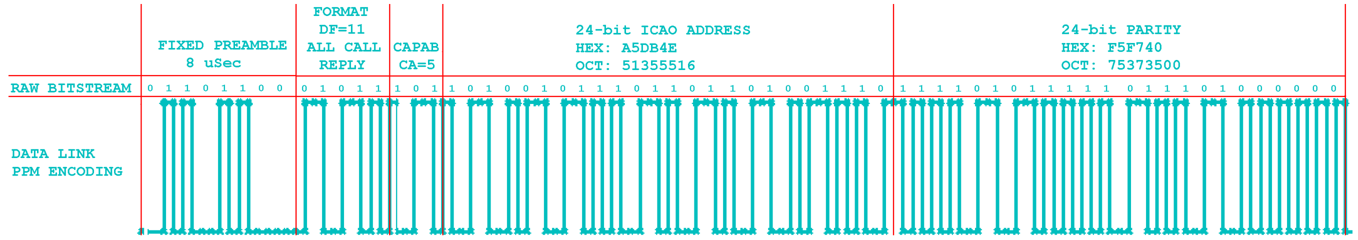

Figure 2. PPM-encoded ADS-B 56 bit sample frame.

probability of existence Mostly observed in intentional or unintentional prankster group, as shown in [46];

2) *Physical Position:*

- *ground-based* - This type of attacker is most commonly presented and envisioned. There are certain limitations which can be used against his/her attacks by various detection and mitigation techniques;
- *airborne* - This type of attacker is still overlooked and perhaps not very well understood and modeled. However, leveraging technological advances, it can include drones, UAV, autonomously activating checked-in luggage or passengers with miniature devices capable of performing attacks;

3) *Goals:*

- *pranksters* - Pranksters seen as least offensive. However, the impact on safety can be considerably higher than assumed. For example, attackers can include unaware pilots, ”curious” and unaware technology experimenters;
- *abusive users* - This type of attackers can have different motivations, including money, fame, message conveying. This can also include privacy-breaching groups (e.g., paparazzi), and eventually pilots intentionally abusing their access to ADS-B technology;
- *criminals* - Such attackers can have two main motivations - money and/or terror;
- *military/intelligence* - Such attackers can have state-level motivation, such as spying, sabotage, etc. and can include agencies related to military or intelligence fields;

B. *Threats*

During the ADS-B introduction, development and deployment, both academic and industrial communities tried to come up with threat and vulnerability models in order to better understand the security impacts and possible mitigation techniques and solutions.

Below is a summary of broad categories of identified and described threats throughout the literature. Details on each particular threat are presented in the subsection V-C.

- jamming, denial of service
- eavesdropping
- spoofing, impersonation
- message injection/replay
- message manipulation

IV. Experimental Setup

A. *Overview*

We took the most straightforward, simple and cost-efficient approach in building up our experimental setup. We deploy a COTS SDR transmitter, which transmits *attacker* controlled messages. The transmitter is controlled by a minimal piece of software, used to encode and control the *attacker* messages. On the receiving end, we use a commercial-off-the-shelf (COTS) receiver, used to confirm the successful reception of the *attacker* messages.

B. *Safety and regulatory considerations*

When doing RF-related research and experimentation, especially related to safety applications such as ATC, it is of utmost importance to abide the regulatory and safety prescriptions. This is to avoid any accidental interference with normal working of the system but also not to use radio frequencies without authorization. Even if the experiment seem perfectly safe, one need to first test it in a controlled lab environment. To avoid any accidental emission of signals, our experimental setup does not emit any radio signals, but simulates any emissions by transmitting signals over a cable directly from the transmitter to the receiver.

To accomplish this without saturating the receiver, we use an inline attenuator, depicted in Figure 3 between our ADS-B OUT USRP1 device, i.e. *attacker*, and our ADS-B IN PlageGadget device, i.e. *victim*. As such our experimental setup does not emit any radio waves. Therefore our setup of *wired* data transmission between ADS-B IN and ADS-B OUT conforms to *Subpart B Unintentional Radiators* of FCC [26].

However, this does not change the results of our experiments as this setup would only require an amplifier and an antenna to actually emit the radio signals.

C. *Hardware*

As our main hardware support, we are using an USRP1 [49] software defined radio device (Figure 4). The USRP is coupled with an SBX transceiver daughter board (Figure 5). The SBX transceiver daughter board [50] covers

Figure 3. Attenuator VAT-10W2+.

Figure 4. Ettus Research USRP1 kit.

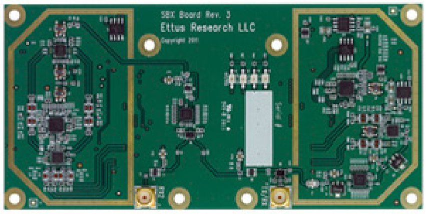

Figure 5. Ettus Research SBX transceiver daughter board.

400MHz-4.4 GHz spectrum range, making a good candidate for 1030 MHz interrogation and 1090 MHz response frequencies. In addition to that, its transmit and receive chains can be controlled separately to provide greater flexibility with scenarios under test.

To assess the correctness of our implementation as well as the effectiveness of the attacks, we use a PlaneGadget ADS-B Virtual Radar [51] (Figure 6). It is a radio-enthusiast-level ADS-B receiver and was chosen because of it's cost vs. characteristics combination. However, there exist currently a large number of choices for radio-enthusiast-level ADS-B receivers [45], any of them could be used in such an experimental setup.

D. Software

1) Overview: As our main software base, we are using the GNURadio [47] open-software package. GNURadio is a FOSS implementation of various radio primitives useful for higher-level designs and applications with SDRs. In particular, it provides very good software support for USRP1 and USRP2. We are using the USRP hardware in Universal Hardware Driver (UHD) mode, which is the recommended one, as it supersedes the original raw device mode.

Figure 6. PlaneGadget ADS-B Virtual Radar.

In addition to using the PlageGadget device as our main ADS-B receiver and decoder, we also use our USRP1 device as a secondary ADS-B receiver, as a backup and verification device. In order to use USRP1 as an ADS-B IN device, it requires demodulation and decoder support. Luckily, there are two public implementations of Mode-S/ADS-B receiver modules for GNURadio. Historically, the first implementation of Mode-S/ADS-B demodulator and decoder was done for pre-UHD-mode by Eric Cottrell [61]. The more recent implementation, which targets the UHD-mode, is done by Nick Foster [62]. Since our USRP1 is in UHD-mode, we are using the *'gr-air-modes'* module [62].

2) Software for the Replay Attack: For this attack, we are using out-of-box functionality of USRP1 and GNURadio, hence on a very high level, our approach looks as:

- capture ADS-B using *uhd_rx_cfile* on 1090 MHz frequency
- for the UHD-mode, use *tx_samples_from_file* to transmit via GNURadio the data captured data to be replayed
- or for the pre-UHD-mode, we use *usrp_replay_file.py* to transmit via GNURadio the data captured data to be replayed

3) Software for Impersonation Attack: For the message impersonation attack, i.e. spoofing, there is a need to implement ADS-B to PPM encoding and PPM modulation modules. As usual, there are multiple ways to implement a solution for this. One of them is by writing a native C/C++-based GNURadio modulator and encoder [63]. Another approach, that we used, is to perform most of the encoding and modulation in MatLab. On a very high level, our is:

- encode high-level ADS-B data into MatLab array as bit-stream representation
- modulate it in PPM in MatLab using *modulate()* function with *'ppm'* argument
- write modulated data from MatLab to I/Q format using *write_complex_binary.m*
- for the UHD-mode, use *tx_samples_from_file* to transmit via GNURadio the data encoded, modulated and written in MatLab at previous step
- or for the pre-UHD-mode, use *usrp_replay_file.py*

For obvious reasons, we cannot present full and final source code, but the following listing should give a general idea of how the encoding and modulation works for simple bit-streams in MatLab:

```
% pulsewidth
pw = 0.5;
% d is data
% 0.5 to (avoid pulse overlap)
d = [ 0 0 1 0 1 0 ] * 0.5;
% sampling frequency
fs = 1e6;
[p, t] = modulate(d, 1000, fs, 'ppm', pw);
t = 0: 1/fs : 1/fs*(length(p)-1);
plot(t, p)
```

V. Discussion

Even though, provisions and specifications exists for a secure mode ADS-B operation, it is currently limited to military use. In addition to this, the specifications of the secure mode ADS-B are not public. Hence, this mode cannot be evaluated and as such analysis of the secure mode ADS-B would be an interesting future work. Military entities have a clear interest in using a secure version of ADS-B, in such a setup it is also easier to secure the communications, e.g., because all aircrafts belongs to the same entity.

Moreover, the commercial air-traffic is prevalent, and as such represents a wider and easier attack surface compared to military secured ADS-B communications.

A. ADS-B Misuses

1) Pranks-like misuse: ADS-B messages allow for freely configured messages which can be set for example by the plane pilot while configuring the ADS-B device. We have found in public sources, e.g., [46], that currently parts of ADS-B messages are used to broadcast various human-readable messages which are unrelated to ATC, ATM or ADS-B, and as such constitute a disguised communication channel over ADS-B protocol. Examples, of such human-readable messages are : VOTENOO, VOTEUNUN, DROPDBRK, GOTOFMS, HIDAD, SCOTSUXX, etc.

While those messages are pranks, this capability can raise several concerns:

- abuses of those messages could carry confusing messages, leading to disturbing pilots from their main task, i.e., conducting airplanes with maximum safety.
- these messages can be seen as hidden, or at least not so straightforward to intercept, information dissemination or hidden call for specific actions.

B. Solutions for securing ADS-B

Along with various existing and proposed solutions, we strongly believe that a lightweight PKI implementation for resource and bandwidth constrained devices, such as aircraft transponders and avionics, is a viable solution for securing ADS-B in the short and long terms. In this context, a possible interpretation for *lightweight PKI* could be that the lengths of keys are much shorter, i.e., adjusted to available bandwidth/bit-rate of the broadcast shared medium, and the computation algorithms are potentially simplified.

The first and simplest thing that would greatly enhance the security of ADS-B is to add integrity verification to ADS-B messages (HMAC and verification). If any certified ADS-B device can securely verify validity of other aircrafts' broadcasts along with verification via CAs chains of the signature keys, the message injection is suddenly not possible or at least not as easy to accomplish. Hence, one approach would be that aircraft A transmits the bits of the signature within each of it's ADS-B messages, in a cycle. After each cycle of N broadcasts, the signature of aircraft A can be gathered by the aircrafts surrounding A. Until, the signature key is totally gathered from broadcasts, the broadcasts from A cannot be verified, thus cannot be fully trusted. However, the surrounding aircrafts would keep these unverified broadcasts messages for later verification, as well as to construct both spatial and temporal constraints of A in order to verify the correctness of the gathered signature key of A, as well as to subsequently verify correctness of data reported by A.

The above would assume and require existence of CAs root keys in the ADS-B transponders in order to verify validity and authenticity of signature keys. We also suggest that key-distribution problem can be overcome from the direction of certification process of avionics devices, specifically ADS-B devices. All avionics devices have to pass various regulatory, safety and other certifications with certifying bodies (FAA, EUROCONTROL, CASA). We suggest that, as part of this certification process, the security integrity check of the hardware/software of the device is executed and the key distribution takes place. In such a PKI process, certificate authorities (CAs) can be designated the certifying bodies, i.e. FAA, EUROCONTROL, CASA, which validate, revoke and update their root certificates on the certified devices during the certification process.

At the same time, enough consideration for lightweight PKI infrastructure and protocols, such as [38], pkASSO [40], LPKI [39], WSN uPKI [41], should be given in order to address PKI challenges faced by globally-distributed ad-hoc network of aircrafts in general, and ADS-B in particular.

Details on each particular solutions from other works are presented in the subsection V-C.

C. Related work

[1] and [2] suggest multiple classification for adversaries, in particular internal vs. external, airborn vs. ground-based, intentional vs. unintentional. A comprehensive classification is made for threats, specifically *Disruption of GPS readings*, *Wireless jamming of surveillance-related communications*, *Exploitation of ADS-B communications*, *Manipulation of ADS-B communications*. As mitigation for ADS-B Position Verification, use of multilateration and radar is proposed; to support ADS-B Message Verification, cryptography techniques are being explored; agains Exploitation of ADS-B communications threats, the idea of *Privacy Mode and Privacy Enhancement for ADS-B* is advanced. As long-term solutions, it is suggested to use *Time Difference of Arrival Multilateration*. As another mitigation factor, the *Group Concept* with extension to *Position Verification by a Group of Aircraft* which is being developed into a *Protocol for Position Verification*.

In [7], authors formulate the possibility of external or internal adversaries to pose threats of ADS-B Message Corruption, ADS-B Message Misuse and ADS-B Message Delay. The proposed mitigations address GNSS Integrity, Integrity of ADS-B OUT Messages, ADS-B Message Anonymity and ADS-B Availability. As long-term solution for the ADS-B, *group concept* is proposed that would be leveraged for ADS-B IN Integrity and ADS-B Privacy.

The above ideas, along with the *group concept* from [7], are continued in [4], under the assumptions of the same type of adversaries. Specifically, primary and secondary surveillance radar infrastructures are proposed for integrity checks and smooth compensation of ADS-B OUT data, with potential enhancement or alternative by using multilateration. For preventing misuse of ADS-B data, a *privacy mode* is proposed, by making the aircraft compute a random identifier as a pseudonym. However, this cannot provide location untraceability when there is a strong spatial and temporal correlation between aircraft locations due to underlying predictable mobility of aircraft and the short intermessage period of ADS-B. Also, it is suggested that symmetric-key-based solutions offers an efficient way to protect integrity, authenticity, and confidentiality, while keyed hash or message authentication code are proposed as message signatures.

McCallie et al. [10] describes a set of attacks such as: *Aircraft Reconnaissance*, *Ground Station Flood Denial*, *Ground Station Target Ghost Inject*, *Ground Station Multiple Ghost Inject*, *Aircraft Flood Denial*, *Aircraft Target Ghost Inject*, and associate each attack a difficulty level and a technique. Of particular interest is that the threats of *Ground Station Target Ghost Inject* and *Ground Station Multiple Ghost Inject* are marked as medium-high, whereas as we currently demonstrate that the difficulty level can be brought down to low-medium. Instead of technical solutions, the paper concludes with four very pertinent recommendations.

Purton et al. [16], uses TOWS and SWOT models to do threat and risk analysis on GPS, ADS-B transmitter, propagation path and ground infrastructure up to and including the ATC display. It also mentions the possibility of the ADS-B spoofing attack. They study security and threats on a broader scale, not just ADS-B. However, the paper doesn't touch the specifics or difficulties associated with ADS-B attacks, mitigations and solution.

Parallel to academic community, hacking community has contributed towards ADS-B insecurity awareness raise with presentations of [42], [43], [44]. Of particular interest is that [44] mentions existence of a private and draft version of a Mode-S/ADS-B native C/C++ transmitter block written for GNURadio, which makes it yet another implementation and proof of the presented attacks.

D. Future work

This research prompts several important ideas for various future work items. Among the most important ones we foresee are:

- security analysis of DF19, DF22 and Mode-5 secure/crypto modes of operation
- development and simulation of a realistic ADS-B security architecture pertaining to the ad-hoc nature and high-mobility challenges of aircraft traffic
- using the USRP-based device to evaluate the security of real certified ADS-B devices, e.g., their resistance to malformed messages, etc.

VI. Conclusion

This paper clearly concludes over the inherent insecurity of the commercial-grade ADS-B protocol design. Despite the fact that lack of security of ADS-B technology has been widely covered by previous academic studies, and more recently by the hacking community, the fundamental architectural and design problems of ADS-B have never been addressed and fixed. Also, given the efforts in terms of time and money invested so far and still to be invested, it is unclear why such mission-critical and safety-related protocol doesn't address at all and doesn't have a security chapter in the main requirements specifications document [19]. As a closing conclusion, the main and intended contributions of our research is awareness raise among academic, industrial and policy-making sectors on the fact that critical infrastructure technologies such as ADS-B require real security in-place in order to operate safely and according to the requirements. We acomplish this awareness raise via this academic exercise by demonstrating that a low-cost hardware setup combined with moderate software effort is enough and sufficient to induce potentially dangerous safety and operational perturbances in a multi-million technology via the exploitation of missing basic security mechanisms such as message authentication at least.

References

[1] K. Sampigethaya, R. Poovendran, L. Bushnell, *Assessment and Mitigation of Cyber Exploits in Future Aircraft Surveillance*, Aerospace Conference (AC), 2010 IEEE

[2] K. Sampigethaya, R. Poovendran, *Visualization & Assessment Of ADS-B Security For Green ATM*, Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th

[3] K. Sampigethaya, R. Poovendran, L. Bushnell, *A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance*, AIAA Proceedings, 2009

[4] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, C. Royalty *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond*, Proceedings of the IEEE, Vol. 99, No. 11, November 2011

[5] K. Sampigethaya, R. Poovendran, *Privacy of future air traffic management broadcasts*, Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th

[6] K. Sampigethaya, R. Poovendran, L. Bushnell, *Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes*, Proceedings of the IEEE, Dec 2008

[7] K. Sampigethaya, R. Poovendran, *Security and Privacy of Future Aircraft Wireless Communications with Offboard Systems*, Communication Systems and Networks (COMSNETS) 2011, IEEE

[8] K. Sampigethaya, R. Poovendran, L. Bushnell, *Secure Wireless Collection and Distribution of Commercial Airplane Health Data*, IEEE Aerospace and Electronic Systems Magazine, 2009, 34(7): 14. 20

[9] L. Kenney, J. Dietrich, J. Woodall, *Secure ATC surveillance for military applications*, Military Communications Conference, MILCOM 2008, IEEE

[10] D. McCallie, J. Butts, R. Mills, *Security analysis of the ADS-B implementation in the next generation air transportation system*, International Journal of Critical Infrastructure Protection, No. 4 (2011), Pag. 7887

[11] J. Krozel, D. Andrisani, M. A. Ayoubi, T. Hoshizaki, C. Schwalm, *Aircraft ADS-B Data Integrity Check*, AIAA Aircraft Technology, Integration, and Operations Conf., Chicago, IL, Sept., 2004

[12] A.C. Drumm, E.M. Shank, *Validation techniques for ADS-B surveillance data*, Digital Avionics Systems Conference, 2002. Proceedings. The 21st

[13] S. Thompson, D. Spencer, J. Andrews, *An Assessment of the Communications, Navigation, Surveillance (CNS) Capabilities Needed to Support the Future Air Traffic Management System*, Project Report ATC-295, 10 January 2001, Massachusetts Institute Of Technology, Lexington, Massachusetts

[14] B. Nuseibeh, C.B. Haley, C. Foster, *Securing the Skies: In Requirements We Trust*, Computer, IEEE Journals & Magazines, Sept. 2009

[15] B. Nuseibeh, C.B. Haley, C. Foster, *Securing the Skies: In Requirements We Trust*, Computer, IEEE Journals & Magazines, Sept. 2009

[16] L. Purton, H. Abbass, S. Alam, *Identification of ADS-B System Vulnerabilities and Threats*, Australian Transport Research Forum, Canberra, October, 2010

[17] Federal IT Dashboard - An Official Website of the United States Government *FAAXX704: Automatic Dependent Surveillance-Broadcast (ADS-B)*, www.itdashboard.gov/investment?buscid=3

[18] Federal Aviation Administration (FAA), *Air Traffic Bulletin, Special Issue 2005-3, August 2005*, www.faa.gov/air_traffic/publications/bulletins/media/atb_aug_05.pdf

[19] *DO-282B, Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance-Broadcast (ADS-B)*, RTCA Paper Number 190-09/SC186-286, RTCA DO-282B, 2009

[20] *DO-249, Development and Implementation Planning Guide for Automatic Dependent Surveillance Broadcast (ADS-B) Applications*, RTCA DO-249

[21] *DO-260A, Minimum Operational Performance Standards for 1090 MHz Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services (TIS-B)*, RTCA DO-260A

[22] *DO-242A, Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)*, RTCA DO-242A

[23] *DO-263, Application of Airborne Conflict Management: Detection, Prevention, & Resolution*, RTCA DO-263

[24] DoT, FAA, Technical Standard Order, *Airborne Navigation Sensors Using The Global Positioning System (GPS) Augmented By The Wide Area Augmentation System (WAAS)*, TSO-C145a

[25] End to- End System Preliminary Hazard Analysis Matrix of Scenarios, *FAA Capstone Safety Engineering Report #1 ADS-B Radar-Like Services*, Volume 2

[26] Electronic Code of Federal Regulations, Title 47: Telecommunication, *PART 15RADIO FREQUENCY DEVICES, Subpart BUnintentional Radiators*,

[27] Surveillance and Conflict Resolution Systems Panel (SCRSP), *Civil-Military Interoperability with Military Mode S Format 22*, SCRSP/WG-A/B, Montreal, 26th to 7th May 2004,

[28] R.D. Grappel, R.T. Wiken, *Guidance Material for Mode S-Specific Protocol Application Avionics*, Project Report ACT-334, Lincoln Laboratory, MIT,

[29] RTCA Special Committee 209 ATCRBS / Mode S Transponder MOPS Maintenance, *Proposed Change to DO-181D and ED-73C for Higher Squitter Rates at Lower Power*,

[30] Jim McMath, *Automated Dependent Surveillance - Broadcast Military (ADS-M)*,

[31] Vincent Orlando, *Extended Squitter Update*, adsb.tc.faa.gov/WG3_Meetings/Meeting1/1090-WP-1-01.pdf

[32] N. O. Tippenhauer, C. Ppper, K. B. Rasmussen, S. Capkun, *On the Requirements for Successful GPS Spoofing Attacks*, CCS11, October 1721, 2011, Chicago, Illinois, USA

[33] E. Lester, J. Hansman, *Benefits and incentives for ADS-B equipage in the national airspace system*, MIT ICAT Report, ICAT-2007-2, 2007

[34] W. Ochieng, K. Sauer, D. Walsh, G. Brodin, S. Griffin, M. Denney, *GPS integrity and potential impact on aviation safety*, The Journal of Navigation Vol. 56, 2003

[35] H.R. Zeidanloo, *Botnet Command and Control Mechanisms*, ICCEE '09, Second International Conference on Computer and Electrical Engineering, 2009

[36] Yuanyuan Zeng, Kang G. Shin, Xin Hu, *Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets*, WiSec'12, April 1618, 2012, Tucson, Arizona, USA

[37] C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, Z. Tianning, *Andbot: Towards Advanced Mobile Botnets*, LEET'11, 4th Usenix Workshop on Large-Scale Exploits and Emerging Threats, 2011, Boston, Massachusetts, USA

[38] A. Khalili, J. Katz, W.A. Arbaugh, *Toward secure key distribution in truly ad-hoc networks*, Proceedings of IEEE Symposium on Applications and the Internet Workshops, 2003

[39] M. Toorani, A. Beheshti, *LPKI - A lightweight public key Infrastructure for the mobile environments*, 11th IEEE Singapore International Conference on Communication Systems, 2008

[40] Ki-Woong Park, Hyunchul Seok, Kyu-Ho Park, *pKASSO: Towards Seamless Authentication Providing Non-Repudiation on Resource-Constrained Devices* , AINAW Advanced Information Networking and Applications Workshops, 2007

[41] B. Kadri, M. Feham, A. M'hamed, *Lightweight PKI for WSN uPKI*, International Journal of Network Security, 2010

[42] Righter Kunkel, *Air Traffic Control: Insecurity and ADS-B*, DefCon 17, Las Vegas, USA,

[43] Righter Kunkel, *Air Traffic Control Insecurity 2.0*, DefCon 18, Las Vegas, USA,

[44] Brad Haines, *Hacker + Airplanes = No good can come of this*, Confidence X, 2012, Krakow, Poland,

[45] *A comprehensive summary of existing radio-enthusiasts-level ADS-B devices*, www.andreicostin.com/papers/AdsbComprehensiveDeviceList.xlsx

[46] RadioReference Community Forum, *Dodgy callsigns from flights*,

[47] GNU Radio, *A free & open-source software development toolkit that provides signal processing blocks to implement software radios*, gnuradio.org

[48] CGRAN, *Comprehensive GNU Radio Archive Network*, www.cgran.org

[49] Ettus Research, *USRP (Universal Software Radio Peripheral)*, www.ettus.com/product/details/USRP-PKG

[50] Ettus Research, *SBX 400-4400 MHz Rx/Tx transceiver daughterboard*, www.ettus.com/product/details/SBX

[51] Radar Gadgets, *Plane Gadget ADS-B Virtual Radar*, www.radargadgets.com

[52] Mini-Circuits, *VAT-10W2+ SMA Fixed Attenuator*, 217.34.103.131/pdfs/VAT-10W2+.pdf

[53] Discovery Tech News, *Iran's Military Hacks U.S. Stealth Drone*, news.discovery.com/tech/irans-military-hacks-us-stealth-drone.html

[54] BBC Tech News, *Researchers use spoofing to 'hack' into a flying drone*, www.bbc.com/news/technology-18643134

[55] SWISS Magazine, *Eco-care reaches new (flight) levels*, May 2012, Pag. 94

[56] NewScientist Tech, *Air traffic system vulnerable to cyber attack*, www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html

[57] USA TODAY 27 May 2011, *Air France jet's final minutes a free-fall*, www.usatoday.com/news/world/2011-05-27-air-france-crash_n.htm

[58] Bureau d'Enquètes et d'Analyses (BEA), *Final Report On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris*, http://www.bea.aero/en/enquetes/flight.af.447/rapport.final.en.php

[59] Garmin, *Garmin GDL 90*, www8.garmin.com/specs/gdl90_0903.pdf

[60] FreeFlight Systems, *Freeflight 1201, 1204, 1203 GPS/WAAS SENSOR SYSTEMS*, www.freeflightsystems.com/docs/FFS_GPS_WAAS.pdf

[61] Eric Cottrell, *GNURadio 'gr-air' module - pre-UHD-mode Mode-S/ADS-B demodulator and decoder*, github.com/russss/gr-air

[62] Nick Foster, *GNURadio 'gr-air-modes' module - UHD-mode software-defined radio receiver for Mode S transponder signals, including ADS-B reports from equipped aircraft*, github.com/bistromath/gr-air-modes

[63] [Discuss-gnuradio] A Chunks to Symbols Related Question, *GNURadio PPM native transmitter block implementation hints*, lists.gnu.org/archive/html/discuss-gnuradio/2012-01/msg00144.html