Experimental Analysis of Attacks on Next Generation Air Traffic Communication

Matthias Schäfer[1], Vincent Lenders[2], and Ivan Martinovic[3]

[1] TU Kaiserslautern, Germany
schaefer@cs.uni-kl.de
[2] armasuisse, Switzerland
vincent.lenders@armasuisse.ch
[3] University of Oxford, UK
ivan.martinovic@cs.ox.ac.uk

Abstract. This work studies the security of next generation air traffic surveillance technology based on Automatic Dependent Surveillance – Broadcast (ADS-B). ADS-B is already supported by a majority of international aircraft and will become mandatory in 2020 for most airspaces worldwide. While it is known that ADS-B might be susceptible to different spoofing attacks, the complexity and impact of launching these attacks has been debated controversially by the air traffic control community. Yet, the literature remains unclear on the requirements of launching ADS-B attacks in real-world environments, and on the constraints which affect their feasibility. In this paper, we take a scientific approach to systematically evaluate realistic ADS-B attacks. Our objective is to shed light on the practicability of different threats and to quantify the main factors that impact the success of such attacks. Our results reveal some bad news: attacks on ADS-B can be inexpensive and highly successful. Using a controlled experimental design, we offer insights from a real-world feasibility analysis that leads to the conclusion that any safety-critical air traffic decision process should not rely exclusively on the ADS-B system.

Keywords: NextGen, ADS-B, Attacks, Security, Threats, Air Safety

1 Introduction

Air traffic control (ATC) systems face large challenges in modern civil aviation. Controllers have to separate an increasing number of aircraft in their airspace. The European Organisation for the Safety of Air Navigation (EUROCONTROL) predicts almost a doubling of instrument flight rules (IFR) movements between 2009 and 2030 [1], which means higher air traffic density and therefore higher separation complexity. At the same time, civil aviation faces an increasing risk of terrorist or other attacks, necessitating protection.

To reliably meet separation minima, i.e. to manage the distances of aircraft to each other, controllers need accurate information about position, velocity and heading of all aircraft in their airspace. This information is retrieved from different sources such as flight progress strips, direct radio communications with the pilot and – most importantly – radar systems [2].

Conventional radar systems can be classified in primary surveillance radars (PSR) or secondary surveillance radars (SSR). PSRs are independent and do not require cooperation of aircraft. They transmit high-frequency signals that are reflected by the target. By receiving and evaluating the resulting echoes, the range, angular direction, velocity and even the size and shape of a target can be determined [3]. To meet higher demands in accuracy, SSR relies on transponders in aircraft, which respond to interrogations by ground stations. The responses contain the precise altitude and other information such as identification codes or information about technical problems. While SSR is still independent, it requires cooperation from the aircraft to function properly.

Driven by the ever growing air traffic volume and the shortcomings of PSR and SSR (mainly accuracy and cost), several efforts are underway to develop a new air traffic surveillance system that relies on satellite based navigation systems (NextGen in the US and SESAR in Europe [4, 5]). The automatic dependent surveillance broadcast system (ADS-B) represents the most prominent system that has been mandated by EUROCONTROL in Europe and the FAA in America. In ADS-B, aircraft continuously determine their own position based on on-board navigational systems (e.g. GPS) and periodically broadcast it to surrounding ground sensors and aircraft. In contrast to PSR and SSR, the ADS-B system is not independent and requires full cooperation of the aircraft.

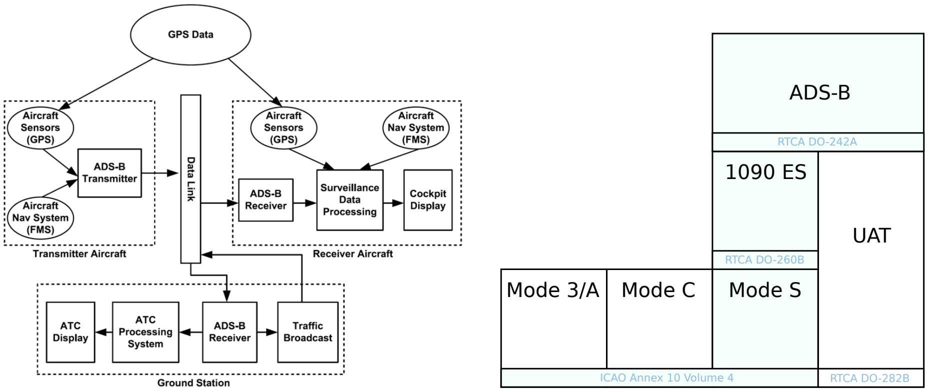
ADS-B support will be mandatory by 2020 in most airspaces in the world. Countries such as Australia and Canada have already started deploying ADS-B ground sensors at a nation-wide scale. By now, most airlines have reacted to this mandate and updated their aircraft with ADS-B capabilities. However, most aircraft manufacturers target a complete equipage by 2020.

ADS-B has evolved out of technologies whose development dates back to World War II. Back then, the designers did not have a modern adversarial model in mind. This deficiency led to a lack of modern security mechanisms and makes the air-ground data link vulnerable to multiple attacks. Even though the security threats and vulnerabilities of ADS-B have been identified and discussed by air navigation safety organizations [6, 7] and open literature [8, 9] for years, the common belief is still that existing vulnerabilities are difficult to exploit because doing so requires high-end equipment and precise positioning of the attacker. Recent research on security of ADS-B considers the difficulty to launch message injection and deletion attacks to be medium to hard [10, 11] because the attacker must craft and transmit valid ADS-B messages.

In 2010, the FAA released the findings of its security certification and accreditation procedures [6]. This report includes comments from various entities, including the U.S. Department of Defense, expressing concerns that parties could monitor transmissions, that broadcasts could be used to target and harm aircraft, and that timing signals could be subject to interruption. However, the FAA concludes that "*using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today*".

These statements, however, mostly rely on qualitative and subjective assessments of the authors or of interviewed people. Considering the technical progress made in the past decades, such as the availability of low-cost software-defined radios, the above statement might underestimate the capabilities of a realistic wireless adversary.

Only recent publications at the computer security events Black Hat 2012 [12] and DEF CON 2012 [13] took practical feasibility of attacks with modern



(a) ADS-B System Architecture [10]   **(b)** Specification hierarchy of ADS-B

Fig. 1: ADS-B Overview

equipment into account. While these publications brought the ADS-B security issues to a wider attention, they did not offer much insights in the threat model.

Hence, the goal of this paper is to take a scientific approach to systematically evaluate the sophisticated ADS-B attacks, in particular those that result in malicious manipulation of radar screens based on injecting ghost aircraft, modifying an aircrafts position, or deleting the presence of an existing aircraft. To provide basic means for the development of countermeasures based on a realistic wireless adversary, we identify constraints an attacker faces under the special conditions of ADS-B. Instead of considering the limits for individual attacks, we break the attacks down into a few basic attack primitives and theoretically derive limits on placement and timing given by the large distances, message formats, and signal propagation characteristics.

Since ADS-B will only be globally deployed and adopted in 2020, the impact of the analyzed attacks on real-world air traffic safety can only be speculated today. Nevertheless, we hope that the insights of this paper will serve responsible authorities to better asses the security risks related to attacks on ADS-B and to be considered in the ongoing deployment and wide-scale adoption of ADS-B.

2 Background on ADS-B

The automatic dependent surveillance broadcast system (ADS-B) is a new paradigm to monitor the airspace and the FAA refers to ADS-B as the satellite-based successor of radar [4]. An overview of the ADS-B system architecture is shown in Figure 1a. In ADS-B, every aircraft computes its own position via on-board GPS and broadcasts it in periodic position messages. These messages are recorded by ground sensor stations and other aircraft in proximity. The broadcasted messages may also contain other fields like velocity, identification, intent, urgency code, and uncertainty level. Each ADS-B equipped aircraft or vehicle automatically starts determining and broadcasting its position and velocity when moving. Depending on the equipment class, the aircraft additionally broadcasts intent information once it enters the en route airspace. Receiving subsystems are used to monitor ground traffic and detect conflicts when moving on the runway. In en route airspaces, aircraft and ground sensors use ADS-B for situational awareness.

2.1 1090 ES Data Link

The ADS-B specification mainly describes the function of broadcasting information. Two standards are proposed as data link. The first alternative is the Universal Access Transceiver (UAT). UAT is specifically designed for ADS-B and other aviation services (e.g. traffic information broadcasting service) to overcome constraints of legacy systems. It establishes a channel with a data rate of 1 Mbps and operates at 978 MHz. Because UAT requires aircraft to be equipped with new hardware (transceivers), the FAA decided to use UAT only in general aviation[4] which is also practice in Europe [6].

For scheduled air transportation, ADS-B uses a mechanism of SSR Mode S, so called extended squitter, to broadcast the aircraft's state vector on the 1090 MHz channel. This combination of ADS-B and Mode S Extended Squitter is also referred to as 1090ES ADS-B (see Figure 1b). Typically, the ADS-B function is directly included into Mode S transponders. As 1090ES ADS-B is the major data link for scheduled air transportation, we focus our security investigations in this work on this standard and do not consider UAT any further.

3 Attacks on 1090ES ADS-B

As there are no cryptographic mechanisms implemented in the ADS-B protocol, messages can be trivially injected, modified or deleted by an attacker who has full control over the wireless channel in a Dolev-Yao [14] manner. However, as shown later, there are several hurdles to overcome for real-world attackers.

3.1 Passive Attacks

An inherent characteristic of wireless networks is the broadcast nature of RF communication. Since ADS-B messages are not encrypted, they can be recorded by an adversary and misused to obtain unique identifiers of aircraft as well as accurate position trajectories. Besides commercially available ADS-B receivers[5], there are even services available on the Internet[6] which provide digitized live ADS-B data to the public. For more sophisticated traffic analyses, there is e.g. a Mode S and ADS-B capable open-source GNU Radio module[7] available. We extended this receiver to eavesdrop and analyze ADS-B traffic and signals.

The FAA argues in [6] that using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today without ADS-B. Yet, privacy concerns are addressed partially by an identifier-based mechanism that provides pseudonymity for ADS-B communication. Furthermore, particular active attacks rely on the knowledge derived by passive eavesdropping of ADS-B messages, i.e. eavesdropping is often the first step involved in active attacks. By combining ADS-B provided data with other publicly available data sources (e.g. official databases provided by aviation authorities), attackers can retrieve enough information to launch targeted attacks. Table 1 shows information on a random aircraft retrieved from ADS-B and publicly available sources.

[4] General aviation refers to all civil flights not belonging to scheduled air transports

[5] http://www.kinetic-avionics.co.uk/

[6] http://www.flightradar24.com/

[7] https://www.cgran.org/wiki/gr-air-modes

Call sign	XYZ
ICAO ID	XYZ
Country	XYZ
Position	XYZ
Altitude	37700,ft
Heading	144°
Speed	395 kn
Climbing rate	896 ft/m

(a) ADS-B

Flight No.	XYZ
Owner	XYZ
Start	XYZ
Destination	XYZ
Scheduled arrival	19:25
Aircraft Model	Airbus A320-214
Seats	126-168
Engine	CFM56-5B4/P

(b) Publicly available sources

Tab. 1: Example information about an aircraft provided by ADS-B and publicly available sources

To get an idea of how much information an attacker could retrieve from eavesdropping ADS-B traffic, we conducted a one week measurement. The receiver was placed on top of a four-storied office building in an urban environment with an airport nearby.

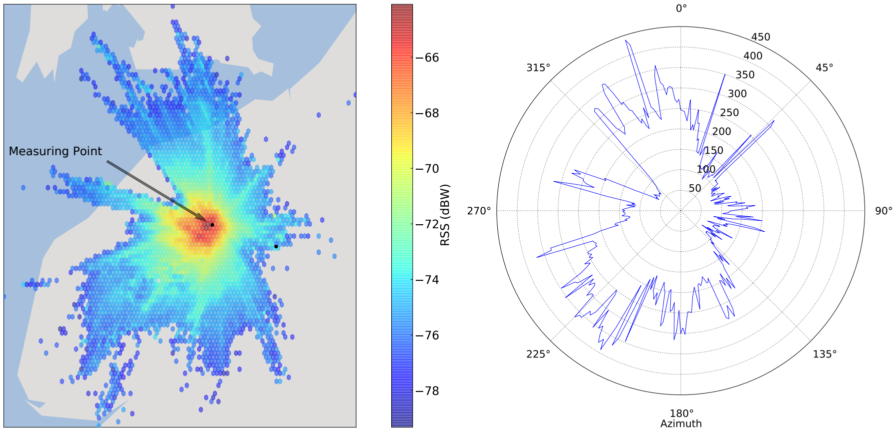
In this week, we have seen 18545 flights of 3041 different aircraft from different countries. Some of these aircraft crossed our reception range in up to 10 flights in one day on their flights back and forth between national airports. On average, each aircraft was visible for roughly 10 minutes. We observed nearly every kind of aircraft ranging from light (< 7031 kg) to heavy aircraft (> 136078 kg), high vortex, high performance (> 5 g acceleration) and high speed (> 400 kn) aircraft, gliders and rotorcraft. By doing long-term measurements over large areas, attackers can derive statistics about persons, airlines or companies. For instance, detailed statistics about destinations, delays or fleet can be used to maintain useful datasets about competitors and their business activities. In addition, we were able to create the Received Signal Strengh (RSS) map shown in Figure 2a with our dataset. RSS profiling-based localization techniques (see e.g. [15] for details) or multilateration can be used to locate aircraft, even if they conceal their position as in case of military aircraft.

Our measurements conclude that the reception quality and range with low cost equipment is remarkable. By positioning our receiver on the roof of a seven-floor building in another experiment on a day with optimal clear weather, we were able to receive messages over distances of up to a maximum of 450 km (compare Figure 2b). This shows that it is easily feasible to monitor the ADS-B traffic of hundreds of aircraft at the same time with a single low-cost receiver.

3.2 Active Attacks

While passive attacks are mainly affecting privacy and might not result in severe risks for air-traffic safety, this section focuses on our main threat model, which is an active attacker. In the following we describe active attacks that may result in severe threats to air traffic safety including attacks on air traffic monitors and automated assisting systems like collision avoidance (TCAS) and pilots.

It is important to keep in mind that we consider ADS-B only, i.e. not in combination with other surveillance technologies. More complex attack scenarios which include combined attacks on several technologies simultaneously are imaginable but beyond the scope of this paper. Furthermore they would require



(a) RSS-based heat map of all position reports (map is randomized)

(b) Reception range in km

Fig. 2: Signal strength and range of our measurements.

detailed knowledge of the actual implementations of surveillance systems, which are apparently kept under tight wraps by the respective authorities.

Attacker Model: The following active attacks are based on three basic attack primitives: message injection, message deletion and message modification. For now, we assume that the attacker has full control over the wireless communication channel and is able to *inject, delete and modify* any ADS-B message. Functional and timing requirements will be derived in Section 5.

Ghost Aircraft Injection: Based on fake message injection, ADS-B messages of a non-existing (ghost) aircraft are broadcasted on the ADS-B communication channel. This attack was presented conceptually in [9–11]. Target of this attack could be any legitimate ADS-B receiver. The ghost aircraft should have realistic properties (position, velocity, ID) in order to be indistinguishable from real aircraft without additional information sources. On the ground, air traffic controllers could be confused or distracted by ghost aircraft. Ghost aircraft could appear as both, taxiing and flying aircraft and combined with poor visibility, this could force controllers to deny landings or instruct aircraft to change their altitude and/or course unnecessarily. In the air, on-board ADS-B-based collision avoidance systems offer attackers a simple way to distract pilots. Again, with poor visibility, pilots primarily make decisions based on their instruments what makes them vulnerable to malicious interference. Deep knowledge about the behavior of collision avoidance systems and a systematic injection of ghost aircraft enable attackers to force collision avoidance systems to instruct pilots to change their course, velocity and/or altitude almost arbitrarily. The injection of ghost aircraft would not directly result in a crash since pilots still make their own decisions. But due to the increased situational complexity, this attack could result in life threatening decisions made by confused pilots and controllers.

Ghost Aircraft Flooding: Based on the same techniques as the previous attack, i.e. message injection, ghost aircraft flooding is the injection of multiple aircraft simultaneously [10]. This attack aims primarily at a denial of service of the controller's surveillance system. Contrary to single ghost aircraft injections, this attack is obvious. By using realistic ghost aircraft, the presence of ghost and real aircraft are hard to distinguish for controllers. The impact of flooding an airborne aircraft with ghost aircraft is unclear, since no tests with collision avoidance systems are reported so far and the detailed implementation of ADS-B-based collision avoidance systems is not publicly available. On the ground, both, airport and airspace surveillance systems can be a target. By covering the airport or airspace with ghost aircraft, management of runways or airborne aircraft is impossible without the support of other surveillance technologies.

Virtual Trajectory Modification: This new attack aims at modifying the trajectory of an *existing* aircraft, which broadcasts correct ADS-B position reports. The attack can be implemented in two ways: by combining message deletion and injection or directly via message modification technique. The former variant deletes all position reports of the target aircraft and replays them slightly modified. The latter variant modifies the position reports in the air. This attack benefits from inaccuracies of other surveillance technologies like primary surveillance radar (PSR), since a tolerant data fusion with e.g. ADS-B and PSR provided data might not reveal these slight inconsistencies. With a smooth takeover, this attack might remain undetected and could lead to wrong instructions by air traffic controllers or delayed reactions of collision avoidance systems.

False Alarm Attack: Similar to the virtual trajectory modification, the attacker deletes and re-injects or modifies messages of a real aircraft in order to indicate a fake alarm. Like Mode S, ADS-B provides mechanisms to indicate emergencies or unlawful interferences such as aircraft hijacking. Such an attack results in confusion and focuses the attention of responsible persons on the target aircraft. Furthermore it may initiate other processes such as the denial of the permission to land or penalty charges for airlines. The detection of this deception on higher levels than the physical layer is hard, since e.g. voice radio must be considered to be untrustworthy in case of a hijacked aircraft.

Ground Station Flooding: Continuous jamming attacks on a ground sensor or aircraft result in high losses and deletion of messages. ADS-B-based ATC cannot provide service any more due to failure of communications. The threat of this attack is well-known [9, 11, 10] and considered to be of low difficulty. This attack would force ATC to switch to other, less efficient or less accurate surveillance and control methods. Especially in high density areas (e.g. around major international airports), a sudden failure of the surveillance or collision avoidance systems is described as *devastating* by controllers and could result in confusion and human failure with fatal consequences. ATC would have to redirect aircraft blindly into other airspaces via voice radio – assuming that voice radio is not attacked as well. If the attacker is strong enough to also jam the communication between aircraft, collision avoidance systems would fail. As history has shown, without the support of collision avoidance systems, collisions are likely to happen. Especially in climbing or descending phases since pilots might miss nearby aircraft due to their limited perspective.

Aircraft Disappearance: Failure of collision avoidance systems and confusion at ground sensors when correlating several data sources can be caused by deleting

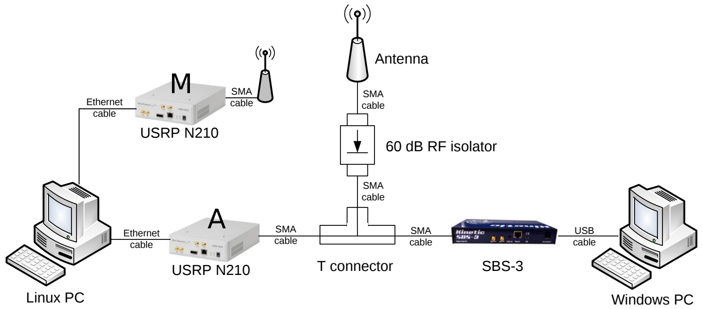


Fig. 3: Experimental setup with additional safety precautions. The attacker's target is an SBS-3 ADS-B receiver which is connected to an isolated antenna and the attacker's signal output. Just in case of a signal leakage, the attacker uses an additional receiver to detect the leakage and terminate the attack immediately.

all messages of a target aircraft with message deletion techniques. By doing so, the attacker prevents aircraft from being detected by ADS-B ground stations or other aircraft. This attack is similar to ground station flooding but more subtle, since the absence of a single aircraft is – if detected – more likely due to failure of avionics than of ground station hardware. If detected, this attack could force the target aircraft to land for safety checks. In case of the attack remaining undetected, the aircraft is not protected by ADS-B-based systems such as collision avoidance, what could have fatal consequences.

Aircraft Spoofing: In order to spoof and outflank surveillance facilities, the ICAO 24 bit address may be spoofed. This can be achieved through combining message deletion and message injection. In addition, the ICAO address in transponders can be reprogrammed by any person who is able to access the cockpit. Masquerading as a friendly aircraft reduces causes for alarm when an unexpected aircraft is detected by other surveillance technologies like PSR.

4 Implementation, Demonstration & Results

This section demonstrates the ghost aircraft injection, ghost aircraft flooding, ground station flooding and virtual trajectory modification attacks with COTS hardware. Within a controlled environment, we were able to launch these attacks in a realistic manner.

4.1 Safety Precautions & Hardware Setup

Due to the criticality of this topic and the legal requirements concerning usage of wireless channels, a safe and yet realistic practical evaluation of the above attacks poses special challenges. At first and most important, all experiments *must not* affect real systems in any way. It must be ensured that none of the attacker's signals can be perceived by a real system. At the same time, a realistic evaluation requires that the attacker's signal underlies realistic channel characteristics including noise and ADS-B traffic from other aircraft.

To fulfill both requirements, we used in consultation with the respective regulatory authority the experimental setup depicted in Figure 3. The target of our attacks was an SBS-3 ADS-B receiver which receives real ADS-B messages via an antenna and forwards them to a PC running a special radar-style visualization software (Kinetic Avionic's BaseStation). The attacker consists out of an off-the-shelf Linux-based PC and an Ettus' USRP N210 SDR (A). To ensure that the attacker's signals do not interfere with real communications, we connected a 60 dB RF isolator ahead of the antenna which attenuates signals unidirectionally in the direction of the antenna. By additionally reducing the transmission power of the attacker's USRP to the least possible value, the signal emitted by the antenna should be imperceptible by any other receivers than our SBS-3 receiver.

As an additional safety precaution, the attacker's PC is connected to a second USRP N210 (M) which runs a GNU Radio-based ADS-B receiver. For the case of an unexpected leakage of the attacker's messages, this receiver is programmed such that it terminates all attacks immediately on reception of a message sent by the attacker. In order to enhance the sensitivity of this *safety monitor*, we disabled the check for valid CRC checksums.

4.2 Implementation

We used the SDR USRP N210 to inject and receive ADS-B messages and to generate jamming signals. The USRP is connected to a host computer that generates samples and sends the digitalized signal data to the USRP via Ethernet. Then, the USRP shifts the software-generated signal from the baseband to the desired frequency using digital up converters, converts the digital to an analog signal and emits it. Together with the open-source software development toolkit for software radios, GNU Radio, the USRP provides a suitable foundation for our implementations at low-cost ($1800-$2500).

For our attacks, we implemented a signal generator block which enables us to generate arbitrary pulse position modulated messages including the preamble according to [16]. A script written in Python generates arbitrary messages and passes them to the signal generator. It generates IQ-samples that are transported to the USRP via Ethernet. A jammer for message deletion attacks is realized with a Gaussian noise waveform generator that covers the full downlink channel of Mode S. For eavesdropping on messages, we extended the open-source GNU Radio Mode S receiver module[8] such that it stores the decoded ADS-B messages plus signal properties (RSSI, SNR, ...) to a database. To inject realistic ADS-B messages, we implemented a library that simulates arbitrary flights. It calculates the trajectory and all required ADS-B messages at the requested rates.

So as not to decrease the implementation complexity for attacks, we skip further implementation details and will not disclose any part of our source code.

4.3 Results

Ghost Aircraft Injection: Our implementation simulates a flight of an aircraft with a fake identity from a starting coordinate to a target coordinate at a given velocity and altitude. The aircraft disappears after arrival. During the ghost flight, the software generates the respective ADS-B position and velocity reports, each with a rate of 2 Hz, and identification reports at 0.2 Hz, i.e. once in 5 seconds. As Figure 4 illustrates, the radar software of SBS-3 shows our injected ghost aircraft flying inconspicuously from the airport in north east to the airport

[8] https://www.cgran.org/wiki/gr-air-modes

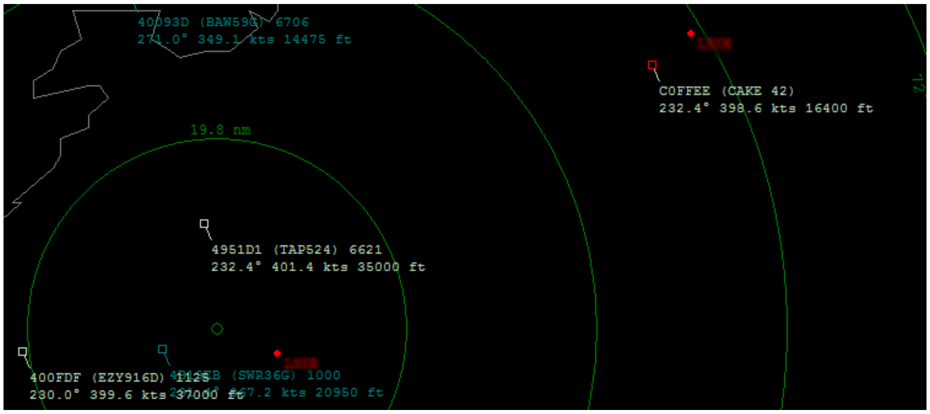


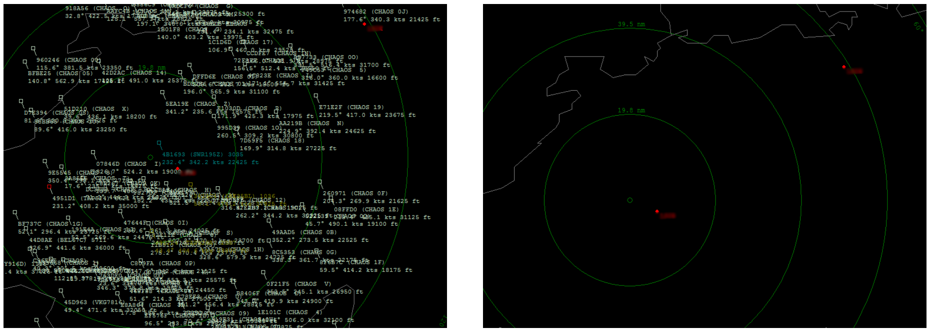
Fig. 4: Ghost aircraft with ICAO 24-bit ID 0xC0FFEE (north east)

in south-west at an altitude of ∼16400 ft and a velocity of ∼400 kn. Except in its obviously fake identifier, the ghost aircraft does not differ from real aircraft.

Ghost Aircraft Flooding: The ghost aircraft flooding implementation generates a given number of ghost aircraft using the ghost aircraft injection implementation but with random (yet realistic) parameters. The starting and target coordinates of each ghost aircraft are set to random coordinates within a target area. The altitude and ground speed are selected randomly from a range between 16400 and 32800 ft and 200 and 600 kts respectively. When starting the attack, all generated ghost aircraft perform simulated random flights back and forth between their start and destination coordinates while sending out the same messages with the same rates as in the ghost aircraft injection above. As Figure 5b shows, this attack results in a complete loss of situational awareness. Due to the random distribution, it is difficult and time-consuming to determine whether an aircraft is real or not. One notable effect of this attack was the freezing of the BaseStation-Software for several minutes due to the heavy workload caused by the high number injected aircraft. Some SSR implementations detect the sudden appearance of targets as a failure of the system and initiate a reboot-procedure, what equals a failure of the system for several minutes. It would be easy for an attacker to cause such a failure if ADS-B receivers are implemented similarly.

Ground Station Flooding: In this experiment, the attacker emits a continuous white noise jamming waveform. This waveform interferences at the SBS-3 resulting in complete deletion of all messages. By executing the attack, the noise level is significantly increased. As Figure 5a shows, a successful reception and demodulation of messages on the 1090 MHz channel is not possible any more, resulting in a complete denial of service.

Virtual Trajectory Modification: We implemented the virtual trajectory modification attack with the combination of the message deletion and message injection attack techniques. First, the attacker deletes all messages at the ground sensor by generating constant interference as in the previous ground station flooding attack. At the same time, the attacker uses an additional ADS-B receiver to capture and forward all but the target aircraft's messages. The forwarded messages are transmitted at a higher power than the interference.



(a) Ghost Aircraft Flooding: 100 randomly distribution ghost aircraft appear in the specified area and fly back and forth between two random coordinates.

(b) Ground Station Flooding: By emitting white noise, all ADS-B messages sent by aircraft in range are destroyed what results in an empty radar screen.

Fig. 5: Snapshots of Kinetic Avionic's BaseStation under Ghost Aircraft Flooding and Ground Station Flooding attacks.

Except for the injected position updates of the modified aircraft trajectory, all aircraft position updates reflect the correct position. The result of this attack was an authentic radar screen (similar to Figure 4) while the trajectory of the target aircraft was modified from the start of our attack. Without any other sources of information, it is hardly possible to recognize this modification since we implemented a smooth takeover.

5 Feasibility and Requirements Analysis

This section provides a better understanding of the actual threat of the eavesdropping, injection, deletion, and modification attack primitives by analyzing their actual requirements under a *realistic* attacker model. In particular, we analyze the timing, positioning and signal power constraints for the attacker and derive practical bounds for these parameters.

5.1 Passive Attacks

The attacker's reception range must include the position of all target aircraft to perform passive attacks. The range depends on the received signal-to-noise ratio (SNR) at the attacker and must satisfy $P_{PA}/N_A > \delta$, where P_{PA} is the received signal power of the aircraft's signal at the attacker, N_A the noise floor of the attacker's receiver, and δ the minimum SNR to correctly decode a message. High gain antennas and a sensitive receiver which is capable of decoding messages with very low SNR can increase the reception range. Another important factor is the position of the receiver. Our experiments showed that obstacles and geographic conditions can reduce the range significantly. Figure 2b illustrates the strong dependency of the range from environmental conditions. A high building at an azimuth of 305° resulted in a massive reduction of the reception range in this direction.

5.2 Active Attacks

All active attacks presented in Section 3 use either message injection, message deletion, message modification, or combinations of these as basic attack mechanisms. This section analyzes the limits of these attack primitives. Especially the signal power, timing and positioning constraints are considered.

Message injection: Since no authentication is required at message level in ADS-B, injecting false messages requires an attacker to implement a transmitter that generates correctly modulated signals in the right message format. Hence, the requirement for a successful message injection attack at ground sensor node G is $P_{AG}/N_G > \delta$, where P_{AG} represents the received power at the ground sensor G emitted by the attacker A, N_G the noise floor at the ground sensor and δ the required minimal SNR to correctly demodulate the signal. For ADS-B receivers that use omni-directional antennas, false messages may be injected from any location as the receiver is not able to discriminate false position messages based on the incoming angle of arrival. However, even when rotating directional antennas are used (e.g. SSR antennas), injecting false messages from a different angle is possible because directional antennas usually have significant side-lobes and will receive the signal even when it does not arrive at the main lobe [17]. The same holds for message deletion and modification attacks.

For attacks that require numerous message injections, the number of messages to be injected is limited by the bandwidth of the channel. The number of injected ghost aircraft is limited by the bandwidth as follows. For 1090 ES ADS-B, each message transmission lasts 120 μs. Assuming each of the n ghost aircraft sends on average m messages per second, n is limited by $n \leq 1\,\mathrm{s}/(m \cdot 120\,\mu\mathrm{s})$. If each aircraft broadcasts its position and velocity with a rate of 2 Hz each and identification once in 5 s, n has an upper bound of 1984. We successfully tested the ghost aircraft flooding attack with this configuration and it turned out that the bottleneck of this attack is indeed the bandwidth of the ADS-B channel.

Message deletion: This attack can be realized in two ways: by means of destructive or constructive interference. With destructive interference, the attacker attempts to annihilate the signal at the sensor by transmitting the inverse of the signal from the legitimate node. As the received signal by the sensor is the superposition of both signals, the resulting signal is erased or at least highly attenuated. This type of interference requires very precise timing and synchronization with the carrier phase and frequency in order to achieve the desired annihilation [18]. This synchronization is hardly achievable with moving aircraft and we will not consider it in this work.

Constructive interference is much easier to achieve as the synchronization requirements are less strict. With constructive interference, the aircraft's signal will experience a higher level of bit errors. The checksum parity field of the extended squitter allows the correction of at most 5 bit errors in a message. Messages with more than 5 bit errors are not correctable anymore and have to be discarded by ground sensors. The requirement for constructive interference at a ground sensor G is

$$\frac{P_{PG}}{P_{AG} + N_G} < \beta, \tag{1}$$

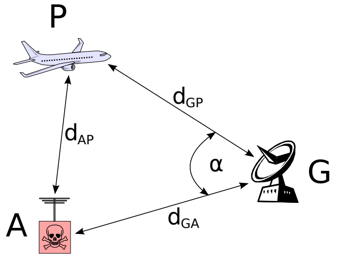


Fig. 6: Attacker Scenario

Deletion decision field	Time offset t_D
ICAO address	40 μs
identification	96 μs
position	96 μs
emergency code	51 μs
positioning integrity (NIC_p)	48 μs
positioning accuracy (NAC_p)	83 μs

Tab. 2: Time offsets for deletion decision in message deletion attacks.

where P_{PG} is the received signal power of the aircraft P's legitimate message and β the threshold for the minimal required SNR to decode messages correctly. The factor β is highly dependent on the signal waveform used by the attacker and how well the receiver is able to suppress this kind of interference with appropriate filters. For a waveform with a white Gaussian distribution with zero mean, the interference can be viewed as noise and β is equal to δ.

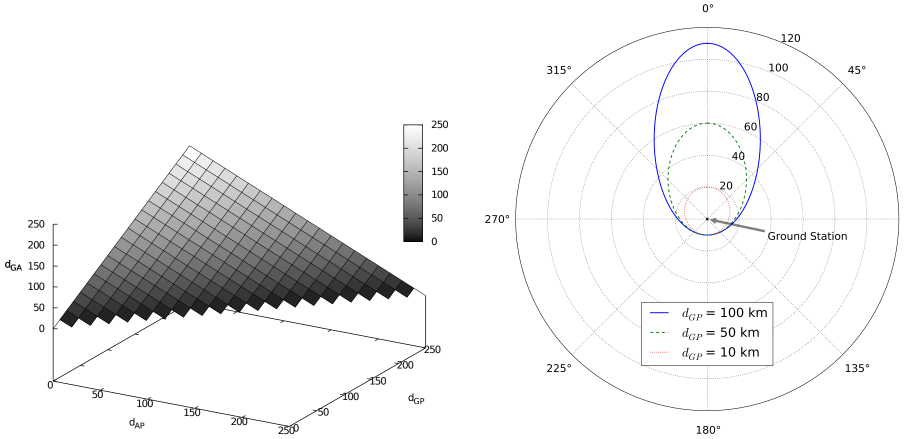
To delete all messages on the channel, requirement (1) is sufficient. However, if the attacker aims at deleting messages selectively, additional timing requirements are given. To delete selected messages, the attacker must continuously listen to the medium, interpret incoming messages, and interfere only with the desired messages before they are completely received at the ground sensor. This form of reactive jamming requires stringent timing in order to hit the message at the receiver. In the following, we derive the timing and placement requirements for this type of selective message deletion.

Let d_{GP} denote the distance between ground sensor (G) and aircraft (P), d_{GA} the distance between ground sensor and attacker (A), d_{AP} the distance between attacker and aircraft, and α the angle between the attacker A and the aircraft P as seen from the ground station G (see Figure 6). Signal propagation speed is assumed to be the speed of light c. The respective signal propagation times t_{GP}, t_{GA} and t_{AP} are then given by

$$t_{GP} = \frac{d_{GP}}{c} \qquad t_{GA} = \frac{d_{GA}}{c} \qquad t_{AP} = \frac{d_{AP}}{c}$$

Let further t_D denote the time offset of the message portion, which is used by the reactive jammer to decide whether it should jam or not, to the first pulse of the preamble. For instance, when an attacker relies on the ICAO 24 bit address of an extended squitter, t_D is $40\,\mu$s[9]. A list of different values of t_D for possible deletion decision fields is given in Table 2. Finally, t_R denotes the reaction time of the attacker, i.e. the hardware switching time between the moment when the decision to delete the message is made until the actual interference is emitted by the attacker. Selective message deletion attacks are then feasible if and only if $t_R < t_{msg} - t_D + t_{GP} - t_{AP} - t_{GA} - 5\,\mu s$ holds, where t_{msg} is the message transmission time (120 μs in this case) and the 5 μs subtracted on the right-hand side results from the minimum of 5 wrong bits required to destroy the messages successfully (due to the CRC). Otherwise, the injected interference would arrive too late at the ground sensor and the intended deletion of the

[9] $8\,\mu$s preamble + $5\,\mu$s downlink format + $3\,\mu$s capability field + $24\,\mu$s ICAO address



(a) Depending on d_{GP} and d_{AP}. Constant parameters are $t_{msg} = 120\,\mu s$, $t_D = 40\,\mu s$ and $t_R = 0\,\mu s$ (worst case)

(b) Depending on the angle α between attacker and aircraft at the ground station. Messages are selected by the attacker based on their ICAO 24 bit ID ($\Rightarrow d_R = 20.09\,\text{km}$)

Fig. 7: Upper bound of the distance d_{GA} (in km) between ground station and attacker for message deletion attacks

message would fail. Due to this, the attacker's position is contrained by $d_{GA} < d_{GP} - d_{AP} + (t_{msg} - t_D - t_R - 5\mu s) \cdot c$. The graph shown in Figure 7a shows an upper bound for d_{GA} when deleting messages based on the aircraft address ($t_D = 40\mu s$) and for a reaction time of zero (worst case). This result shows that this attack always benefits from far distances between ground station and aircraft and short distances between attacker and ground station.

However, the attacker has a clear advantage because he can adjust his position such that the angle α is optimal to him. Assume for example an attacker that is positioned close to an airport. Since all aircraft will land and start along the same direction, he may optimize his attack range without the need to reduce its distance to the ground station. For the attacker's reaction and distance requirements in relation to the angle α, we use the law of cosines and get

$$d_{GA} < \frac{d_R \cdot d_{GP} + \frac{d_R^2}{2}}{d_R + d_{GP} \cdot (1 - \cos\alpha)} \tag{2}$$

where $d_R = (t_{msg} - t_D - t_R - 5\mu s) \cdot c$. Figure 7b shows an upper bound for d_{GA} when deleting messages based on the aircraft address and with zero reaction delay ($t_R = 0$). The curves represent an upper bound on d_{GA} for different angles α and fixed distances $d_{GP} = 100, 50$ and $10\,\text{km}$.

As we see, as long as the attacker is within a radius of about 10 km around the ground station, he may successfully launch the message deletion attack independent of α and the distance of the aircraft to the ground station. For larger distances between the attacker and the ground station, the attacker is better off being in the same direction of the aircraft as seen from the ground station.

Clearly, selective message deletion requires fast reaction times t_R at the attacker in the order of a few microseconds. However, Wilhelm et al. have shown that it is possible to achieve fast jamming reaction times in the order of a few μs with commercial off-the-shelf SDRs such as USRP2 [19]. Considering message rates and using further traffic analysis to predict the emission of messages may relax these constraints on the reaction time to a certain degree at the cost of higher detection complexity.

Message modification: The goal of message modification attacks is to modify a message while it is being transmitted over the air. There are two possible techniques to manipulate messages during transmission — overshadowing and bit-flipping. When overshadowing, the attacker's signal is of such high power relative to the legitimate transmission that the original message (or parts of it) appears as noise. With bit-flipping, the attacker superimposes the radio signal such that one or several bits are converted from one to zero or vice versa. Bit flipping requires precise synchronization to the carrier phase and frequency and is hence extremely difficult to achieve for moving targets like aircraft and is therefore not considered in this work [18].

To overshadow the signal of a legitimate aircraft transmitter, $P_{AG}/P_{PG} > \gamma$ must hold, where γ is a fixed threshold value defining the minimum signal-to-interference ratio (SIR) at which the attacker's signal is decoded without error.

The timing and distance requirements are slightly more strict than for the message deletion attack. Let t_M denote the offset of the message portion to be modified to the last bit of the field that is used by the attacker to decide whether it should modify the actual message or not. For instance, when an attacker wants to modify the sixteenth bit of the message data (ME) field based on the ICAO 24 bit address in the aircraft address (AA) field, t_M is 16 μs since the ME field is directly after the AA field. On-the-fly modification attacks are then feasible if and only if the following constraint on the attacker's reaction time is satisfied:

$$t_R < t_M + \frac{d_{GA} + d_{GP} - \sqrt{d_{GA}^2 + d_{GP}^2 - 2\ d_{GA}\ d_{GP} \cos\alpha}}{c} \tag{3}$$

Otherwise, the injected modification signal arrives too late at the aircraft and the intended modification of the message fails. Due to this, we can formulate the following constraint on the attacker's position:

$$d_{GA} < \frac{d_{GP} + \frac{c}{2} \cdot (t_M - t_R)}{1 + \frac{d_{GP} \cdot (1 - \cos\alpha)}{c \cdot (t_M - t_R)}}. \tag{4}$$

Since a CRC checksum is used to detect transmission errors, the CRC must be further modified by the attacker in any case to preserve the validity of the message. This does not pose a challenge since all transmitted bits are known to the attacker and he is therefore able to calculate the new CRC of the modified message and modify the CRC as well.

An additional timing challenge lies in the estimation of the signal propagation delays t_{GP}, t_{AP}, and t_{AG}. The attacker needs to precisely estimate these delays such that its overshadowing signal arrives at the correct time of the bits to be modified. An overall estimation precision below 1 μs is necessary to inject its modified bit sequence at the correct message position at the ground sensor.

This synchronization is however easy to achieve since the exact positions of the aircraft are known to the attacker from the received ADS-B messages.

To summarize this section, the following statements can be concluded from this section. While message eavesdropping and message injection are only constrained by signal power, the message deletion and message modification attacks have additional constraints with regard to timing and position. Nevertheless, we have shown that these constraints are not major hurdles. An attacker can launch these attacks with low-cost software radio equipment at distances of up to ten km to the ground station independent on the aircraft constellation in the sky. By carefully positioning itself with the correct angle, an attacker may even increase its attack range beyond 100 km from the ground station.

6 Related Work on ADS-B Security

While the aviation community already expressed reservations about the lack of security mechanisms[10], research on ADS-B security as found in the open literature has focused on the identification of vulnerabilities and subjective risk analysis. This section provides a summary of open literature on ADS-B security.

Korzel and Andrisani already identified potential threats resulting from unverified ADS-B reports in 2004 [8]. They proposed verification and validation techniques to verify the reported state of an aircraft, signal conformance in terms of the reported position vs. true physical position and intent conformance. They use a suite of Kalman filters to estimate the state of an aircraft and multilateration to compare signal properties with the reported position. The focus of their work is however not on security aspects and no concrete adversarial model is considered by the authors. In addition, they do not investigate particular threats resulting from the lack of security mechanisms.

In 2007, Valovage discusses several enhancements to ADS-B including security services such as authentication and confidentiality with cryptographic methods [20]. They propose an authentication scheme in terms of pre-shared keys and cryptographic hash sums.

In 2009, Wood interviewed six professionals affiliated with the aviation community [21]. Based on their subjective assessments, they conducted a security risk analysis. The work is focused on three central aspects: comparing the ADS-B network design to government and commercial industry network security standards, identifying several similarities and differences between the introduced ADS-B network and industry standard computer networks. They also analyzed the behavior of ADS-B when faced with common computer network threats such as denial of service, session hijacking, and network eavesdropping attacks. They offer a brief analysis of threats and vulnerabilities concerning confidentiality, integrity and availability of ADS-B. In contrast to our work, the assessments of threats are based on the subjective experience of the interviewed people. Hence, there is no systematic evaluation and feasibility analysis of these threats from a technical perspective.

Sampigethaya et al. identified several attacks in 2010 and proposed solutions based on cooperative groups of aircraft to mitigate threats to airborne surveillance [9, 22]. Furthermore, they designed a security simulation concept and sim-

[10] http://www.airsport-corp.com/adsb2.htm

ulation tool which allows users to model and quantify the impact of ADS-B exploits. However, they do not provide any statements about the feasibility of attacks on the ADS-B data link. The overall objective of attackers in their model is to degrade accuracy and performance, while more sophisticated attacks are not at the focus of their analysis. In 2010, Purton et al. performed an analysis of the threats, opportunities, weaknesses and strengths (TOWS analysis) of the ADS-B system [11]. They identified several threats to different communication links (GPS, propagation path, ground infrastructure), rated their likelihood and severity, and derived strategic actions. They only provide qualitative judgments about likelihood and severity based on the high-level assessments of the authors. Again, no detailed technical investigations are made to provide realistic statements on feasibility of specific attacks. The primary objective of McCallie et al. in their work in 2011 was to establish a taxonomy to classify attacks on ground stations and aircraft based on ADS-B message injection, jamming and interception [10]. Additionally, they provided valuable security recommendations, which request more transparency of security certifications and accreditation procedures, and a complete security analysis of the whole NextGen system design. They motivate the integration of security as an additional objective in SSR development and an adequate education on security aspects to the aviation community. Attacks are considered to be of low difficulty only if specialized hardware and software are readily available. Compared to their work, we see our contribution as an important step forward in understanding the severity of the threats.

7 Conclusion

ADS-B is an air-traffic surveillance technology that will become mandatory for regulating airspace in 2020. One of the main objectives of this technology is to increase the safety of the worldwide air traffic by increasing the aircraft positioning accuracy. The main objective of this work was to investigate practical attacks against ADS-B and to offer insights from a real-world evaluation. We believe that by providing these insights, this work will help ATC and regulation authorities to realistically assess the risks that this technology will pose when fully operational. We conclude that without appropriate countermeasures, critical air traffic management decision processes should not rely on ADS-B derived data. Finally, we hope that the rule makers and regulators involved in the ADS-B standardization process will recognize the criticality of the described threats and include security as one of its key requirements in future releases.

References

1. Statistics and Forecast Service: Long-Term Forecast: IFR Flight Movements 2010 – 2030. EEC Technical Report CND/STATFOR Doc415, EUROCONTROL (2010)
2. Carswell, C.M., ed.: 6: Air Traffic Control. In: Reviews of Human Factors and Ergonomics. Volume 4. Human Factors and Ergonomics Society (2008) 195–244
3. Merrill Ivan Skolnik: Radar handbook. 3 edn. McGraw-Hill Professional (2007)
4. Federal Aviation Administration: NextGen Implementation Plan. (March 2011)
5. SESAR Consortium: The ATM Target Concept. Technical report (2007)
6. Federal Aviation Administration: Automatic Dependent Surveillance—Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Final Rule. Federal Register **75**(103) (May 2010) 14 CFR Part 91.

7. ICAO: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. 9 edn. (2011) Annex 17: Security.
8. Krozel, J., Andrisani, D., Ayoubi, M.A., Hoshizaki, T., Schwalm, C.: Aircraft ADS-B Data Integrity Check. In: AIAA Aviation, Technology, Integration, and Operations Conference Proceedings. (September 2004)
9. Sampigethaya, K., Poovendran, R.: Visualization & assessment of ADS-B security for green ATM. In: Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th. (October 2010) 3.A.3–1 – 3.A.3–16
10. McCallie, D., Butts, J., Mills, R.: Security analysis of the ADS-B implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection **4** (2011) 78–87
11. Purton, L., Abbass, H., Alam, S.: Identification of ADS-B System Vulnerabilities and Threats. In: Australian Transport Research Forum. (October 2010)
12. Andrei Costin: Ghost is in the air(traffic). Black Hat USA (July 2012)
13. Brad Haines: Hacker + Airplanes = No Good Can Come Of This. DEF CON®20 Hacking Conference (July 2012)
14. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Transactions on Information Theory **29**(2) (mar 1983) 198 – 208
15. Mao, G., Fidan, B., Anderson, B.D.: Wireless sensor network localization techniques. Computer Networks **51**(10) (2007) 2529 – 2553
16. ICAO: Annex 10: Aeronautical Telecommunications. 4 edn. (2007) Volume IV: Surveillance and Collision Avoidance Systems.
17. Stevens, M.: Secondary surveillance radar. Artech House (1988)
18. Pöpper, C., Tippenhauer, N.O., Danev, B., Capkun, S.: Investigation of Signal and Message Manipulations on the Wireless Channel. In: European Symposium on Research in Computer Security (ESORICS). (September 2011)
19. Wilhelm, M., Martinovic, I., Schmitt, J.B., Lenders, V.: Reactive jamming in wireless networks: how realistic is the threat? In: Proceedings of the fourth ACM conference on Wireless network security. WiSec '11 (2011) 47–52
20. Valovage, E.: Enhanced ADS-B Research. Aerospace and Electronic Systems Magazine, IEEE **22**(5) (May 2007) 35 –38
21. Wood, R.G.: A security risk analysis of the data communications network proposed in the nextgen air traffic control system. PhD thesis, Stillwater, OK, USA (2009)
22. Sampigethaya, K., Poovendran, R., Bushnell, L.: Assessment and mitigation of cyber exploits in future aircraft surveillance. In: IEEE Aerospace Conference. (March 2010)