# Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B

*Martin Strohmeier, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic*

*Martin Strohmeier and Ivan Martinovic are with the University of Oxford.*

*Matthias Schäfer is with the University of Kaiserslautern.*

*Vincent Lenders is with armasuisse.*

## ABSTRACT

Air traffic is continuously increasing worldwide, with both manned and unmanned aircraft looking to coexist in the same airspace in the future. Next generation air traffic management systems are crucial in successfully handling this growth and improving the safety of billions of future passengers. The Automatic Dependent Surveillance Broadcast (ADS-B) system is a core part of this future. Unlike traditional radar systems, this technology empowers aircraft to automatically broadcast their locations and intents, providing enhanced situational awareness. This article discusses important issues with the current state of ADS-B as it is being rolled out. We report from our OpenSky sensor network in Central Europe, which is able to capture about 30 percent of the European commercial air traffic. We analyze the 1090 MHz communication channel to understand the current state and its behavior under the increasing traffic load. Furthermore, the article considers important security challenges faced by ADS-B. Our insights are intended to help identify open research issues, furthering new interest and developments in this field.

## INTRODUCTION

The air traffic load has experienced tremendous growth over the last decade. The reported average number of registered flight movements over Europe is around 26,000 per day. Large European airports may spike to more than 1,500 daily takeoffs and landings. The tendency is still increasing and forecasts assume almost a doubling of movements between 2009 and 2030.[1] With the growing adoption of unmanned areal vehicle (UAV) technology for civil applications, we may even expect a further boost in air traffic over the coming years.

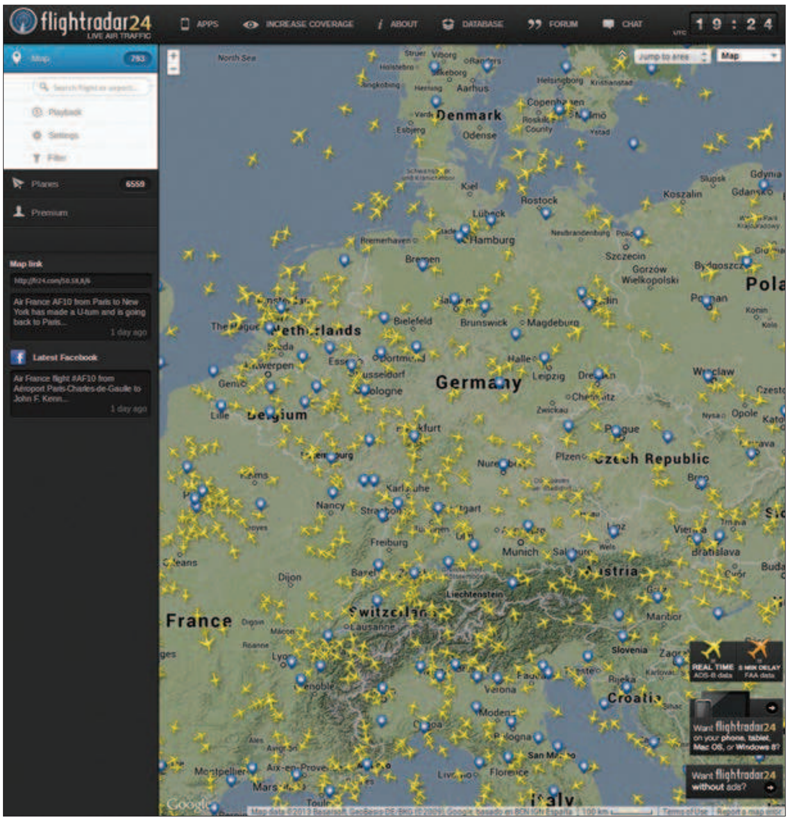
To avoid accidents and collisions in such a dense air space, rules and coordination are fundamental. The worldwide concept for safe navigation is based on a combination of mechanisms for flight separation and collision avoidance. Scheduled flights are all separated by altitude and distance from directives by surveillance personel operating on the ground. Each aircraft is further responsible to detect and avoid potential collisions that may occur despite the allocated separation.

A key feature for both separation and collision avoidance is the ability to continuously localize all aircraft in the sky. The traditional approach for aircraft localization is to rely on radar systems that were originally developed for identification, friend or foe (IFF) systems used in military applications. Such conventional radar systems can be classified in primary surveillance radars (PSR) or secondary surveillance radars (SSR). PSRs are independent and they do not require cooperation from the aircraft. They transmit high-frequency signals, which are reflected by the target. By receiving and evaluating the resulting echoes, the range, angular direction, velocity, and even the size and shape can be determined. In contrast, SSR relies on transponders in the aircraft, which respond to interrogations from ground stations. The response contains precise aircraft height information and other information such as identification codes or information about technical problems which makes it possible to meet much higher demands on localization, identification, and status reports compared to PSR. Since the surveillance data is derived by the aircraft itself, SSR is *dependent*. It also requires *cooperation* from the aircraft to function properly.

An emerging problem with traditional PSR and SSR systems is their relatively low precision and detection accuracy [1]. The increasing traffic density in the sky requires aircraft localization techniques that exceed the inherent limits of these radar technologies. A new technology for air traffic monitoring that holds the promise to achieve the required precision and that is planned to replace conventional radar systems is the Automatic Dependent Surveillance Broadcast system (ADS-B). The idea of ADS-B is to combine satellite-based positioning with a radio frequency (RF) data-link to continuously and

*[1] http://www.eurocontrol.int/sites/default/files/content/documents/official-documents/forecasts/long-term-forecast-2010-2030.pdf.*

0163-6804/14/$25.00 © 2014 IEEE



http://fr24.com/50.18,8/6

Air France AF10 from Paris to New York has made a U-turn and is going back to Paris...
1 day ago

Air France flight #AF10 from Aéroport Paris-Charles-de-Gaulle to John F. Kenn...
1 day ago

**Figure 1.** Live radar picture of ADS-B-equipped aircraft over Central Europe from flightradar24.com.

automatically broadcast location updates and intents, instead of merely responding to interrogations by ground stations. ADS-B has been standardized and the FAA as well as EUROCONTROL have mandated its deployment for 2020 as part of next generation air transportation systems NextGen and SESAR. By then at the latest, all scheduled flights will be required to send continuous location updates with ADS-B capable transponders.

As of today, most airlines have started to equip their fleet with ADS-B transponders in order to be ready when the technology becomes mandatory. As a consequence, a significant portion of the aircraft traffic is already sending out ADS-B signals. Although ADS-B messages are sent unencrypted and anybody may have been capturing those signals for years, we are unaware of any larger field studies providing deeper insights on the technology at a wider scale. While preliminary experiments at airports (e.g. [2]) have been reported, these studies were either limited by the number of stations or the coverage area. A different option for high-level information are live radar services available freely on the Internet which in the meantime offer extensive coverage of worldwide traffic. These services, too, utilize ADS-B data but provide only insights about aggregated flight tracks, illustrating the increasing traffic density (Fig. 1).

This article analyzes the current state of the ADS-B system in a comprehensive large-scale measurement campaign using OpenSky [3], a research sensor network deployed in Central Europe. As of this writing, OpenSky includes eleven sensor nodes geographically distributed over an area of 720,000km$^2$. Over a period of nine months, we were able to capture ADS-B traffic of more than 7,500 flights per day on average, using over 13,500 different aircraft in total; the overall data currently consists of more than 4.5 billion ADS-B messages. Using this realistic and rich source of data, we were able to analyze ADS-B communication characteristics in more detail. With respect to the increasing air traffic in both manned and unmanned aviation, two issues have been identified as relevant problems:

- The ADS-B system is susceptible to severe message collisions in dense air spaces. The random channel access of the communication protocols using the 1090MHz frequency leads to ADS-B packet error rates above 50 percent for typical air space densities as observed during the day.
- Furthermore, we discuss recently identified security concerns surrounding ADS-B. There are practical RF attacks with cheap off-the-shelf software-defined radios. An adversary can inject false aircraft positions or modify the position of existing ones without the receiver being able to notice the presence of these attacks.

With the help of a sensor network, we want to put both of these issues in a real-world context, discussing insights that are valuable for the future deployment of ADS-B. This work focuses on the current state of deployment of ADS-B and potential indicators for future developments.

## Overview of ADS-B

This section provides a short overview of the development of the ADS-B protocol, its history and current applications.

### The ADS-B Protocol

The American Federal Aviation Administration (FAA) as well as its European counterpart EUROCONTROL named ADS-B as the satellite-based successor of radar. Until today, air traffic control (ATC) relies on interrogation-based SSR, so called modes, to retrieve an aircraft's identity and altitude. Table 1 compares the modes A, C, and S, which are in common use for civil aviation. With its creation, ADS-B constitutes a paradigm shift in ATC toward cooperative and dependent surveillance. Every participant retrieves their own position and velocity by using an onboard GPS receiver. This and other information such as ID, intent, urgency code, and uncertainty level are then periodically broadcast in a message (typically twice per second) by the transmitting subsystem called *ADS-B Out*. The messages are received and processed by ATC stations on the ground as well as nearby aircraft, if equipped with the receiving subsystem *ADS-B In*.

There are two competing ADS-B data link standards that have been proposed: Universal Access Transceiver (UAT) and 1090MHz Extended Squitter (1090ES). UAT uses the 978MHz frequency and has been created specifically for use with aviation services such as ADS-B. Since UAT requires fitting new hard-

|  | Message length | Frequencies (MHz) | Operational mode | Use cases |
|---|---|---|---|---|
| Mode A | 12 bit | 1030 (up)<br>1090 (down) | Independent/Non-selective interrogation | Identification |
| Mode C | 12 bit | 1030 (up)<br>1090 (down) | Independent/Non-selective interrogation | Pressure Altitude Extraction |
| Mode S | 56/112 bit | 1030 (up)<br>1090 (down) | Independent/Selective interrogation | Multiple |
| ADS-B/1090ES | 112 bit | 1090 | Dependent/Automatic | Multiple |

**Table 1.** Comparison of civil aviation transponder modes.

ware, it is currently only used for general aviation in EUROCONTROL and FAA-mandated airspaces. Commercial aircraft employ a revamped version of the traditional SSR protocol Mode S. This so called Extended Squitter operates on the 1090MHz frequency and is a combination of ADS-B and Mode S. In other words, the ADS-B function can be integrated into existing Mode S transponders. Figure 2 provides a graphical illustration of the ADS-B system architecture and the protocol hierarchy.

From here on, we focus on the commercially used 1090ES data link. The complete technical overview of the ADS-B protocol can be found in the specification documents [1, 4]; various other works give succinct, higher level descriptions of the protocol (e.g., [5]).

### Development and Use Cases

While there were a number of reasons behind the switch to a modern air traffic management system, cost has consistently been mentioned as one of the most important throughout the process; existing radar infrastructures are much more expensive to deploy and maintain [6] compared to ADS-B. Furthermore, it provides significant operational enhancements for airlines and air traffic managers. The increased accuracy and precision should improve safety and decrease the likelihood for air traffic incidents by a large margin. Furthermore, pilots profit from enhanced situational awareness in their cockpits.

Industry and regulators estimate that in 2013 more than 70 percent of all commercial aircraft worldwide were already equipped with ADS-B transponders [7]. Countries such as Australia and Canada have already deployed full continental coverage, with ADS-B sensors being the single means of ATC in low population areas of the country.

ADS-B was developed to address some main use cases:

**Airport Control**:
- Runway control/taxiing: GPS-based localization improves the handling of aircraft on the ground where very high precision is needed.
- Approach/take-off: Improved accuracy increases ATC safety and makes it possible to reduce the density of approaches and take-offs at busy airports, leading to significant cost reductions.

**En-route ATC**:
- Wide-area regions: ADS-B enables and significantly reduces cost for full en-route coverage of flights in very low-density regions such as the vast open spaces in Canada or Australia.
- Collision Avoidance: Improved localization benefits Traffic Collision Avoidance Systems (TCAS) and reduces the danger of mid-air collisions. Modern TCAS systems can utilize ADS-B messages to improve performance.
- UAV Sense and Avoid: Control and collision avoidance for UAV is shifting to Sense and Avoid (SAA), permitting the UAV to self-separate from potential obstacles.

## ADS-B Deployment in Central Europe

There are many successful community projects utilizing ADS-B, such as websites offering live radar services based on commercially available hardware. These projects provide high-level data and the abstract content of received ATC messages. While this is highly useful, a low-level view on ADS-B and its frequency is needed to conduct a thorough full-scale analysis of the current state of deployment. Besides purpose-built hardware, modern software-defined radios with specialized software provide a cheap and flexible way to collect large amounts of ATC-related data.

We use OpenSky, a sensor network consisting of 11 sensors located in Central Europe, to collect ADS-B messages on a large scale. In OpenSky, all ADS-B messages received from aircraft over the 1090ES data link are stored. We rely mainly on commercial SBS-3 stations from Kinetic Avionics as sensors to collect these messages. Since SBS-3 does not report a received signal strength indicator (RSSI), we also use a special-purpose software-defined radio receiver for ADS-B, based on USRP products in combination with the GNU Radio project, to enhance data collection. Gathering additional information such as RSSI and signal-to-noise ratio (SNR) allows us to conduct a more thorough analysis. For more information on OpenSky, see [3].

Our collected data shows that despite ADS-B being only slowly rolled out and still in the test-

*Industry and regulators estimate that in 2013 more than 70 percent of all commercial aircraft worldwide have already been equipped with ADS-B transponders [7]. Countries such as Australia and Canada have already deployed full continental coverage, with ADS-B sensors being the single means of ATC in low population parts of the country.*

ing stage, a majority of commercial flights over Central Europe has already adopted the standard. On average, about two-thirds of all aircraft that crossed the receiving range of our network broadcast ADS-B messages. Since our sensor network went online on 31/01/2013, we have seen around 13,000 aircraft from 98 different countries (see also Table 2). Most aircraft were from Germany (19.03 percent), the United Kingdom (11.58 percent), and the United States (11.49 percent), followed by Switzerland (6.63 percent), Ireland (6.55 percent), and France (6.23 percent). Approximately 7,500 flights cross our reception range every day, even though not all aircraft are even equipped with ADS-B yet and we only monitor Central Europe as of now. Yet this constitutes already approximately 30 percent of the overall commercial flight traffic in Europe, where EUROCONTROL records 25,000–30,000 flights per day depending on the time of year.

### Message Types and Rates

Many aircraft have not yet fully implemented the ADS-B standard. Ninety-eight percent of all ADS-B equipped aircraft that crossed our network's range at least broadcast their call sign; 80.4 percent reported their position; 79.2 percent reported their velocity. All three message types are broadcast by 76.9 percent. Miscellaneous messages, including unknown formats as well as test messages, were sent out by 27.4 percent of aircraft, making up less than 3 percent of all received messages.

Position and velocity are each broadcast twice per second and the call sign once in five seconds. Combining these three message types, an average aircraft can therefore be assumed to currently have an ADS-B message rate of 4.2 messages per second. This will increase to 6.2 messages per second and more when other types such as periodic status messages are implemented in the future [1].

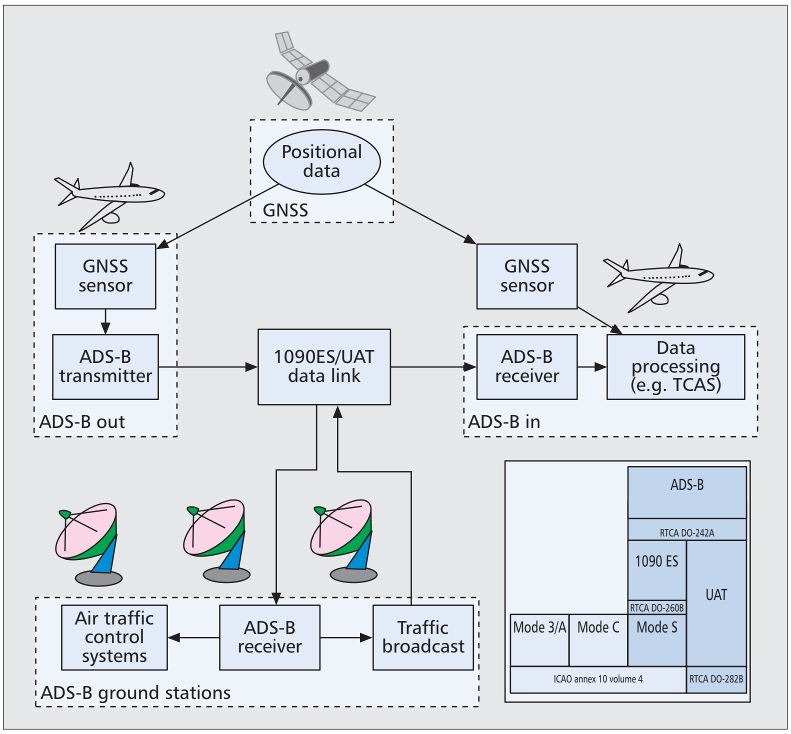


**Figure 2.** ATC system architecture and protocol hierarchy [3]. The positional data provided by the satellite navigation system is processed by the aircraft and broadcasted through the ADS-B Out system alongside other situational information. ATC ground stations and other aircraft (via ADS-B In) receive these messages over the 1090 ES or UAT data link.

| Online since | 31/01/2013 |
|---|---|
| Sensors | 11 |
| Received messages | > 4,500,000,000 |
| Flights per day | ca. 7,500 |
| Different aircraft | ca. 13,000 |

**Table 2.** OpenSky statistics as of February 2014.

## Analysis of the ADS-B Channel

We used a sample of 53,626,642 messages recorded over a 14-day period with a USRP-based receiver to conduct an in-depth analysis of the ADS-B channel characteristics.

### Loss and Channel Quality

As an indicator of the channel quality, the signal-to-noise ratio (SNR) of correctly decoded messages ranged from 2.71dB to 33.13dB, with the 0.5 and 99.5 percent quantiles at 7.64dB and 21.79dB, respectively. Messages with an SNR higher than about 16dB were highly likely to be decoded correctly.

In all our measurements, we noticed that we received considerably fewer ADS-B messages than we should have according to the specification and the observed aircraft behavior. The message loss rate was much stronger than could be attributed to weather or other external influences. In looking for the causes, Fig. 3 shows the impact of several variables on the percentage of packets lost at the receiver. Figure 3a illustrates the loss rate against the distance of the aircraft from the receiver. For the most part, we can observe slow linear growth of the mean from 30 percent at 50km to 50 percent at approximately 280km. However, there are two noticeable effects: message loss accelerates significantly past the 280km mark, and message loss is actually higher (up to 40 percent) below 50km.

On top of this typical signal behavior, we noticed that loss rates correlate with the time of day, as seen in Fig. 3b. The loss rates are significantly lower in the morning and in the evening, i.e. in off-peak traffic times when considerably fewer aircraft are in transmission range. Following this pattern, Fig. 3c shows the effect against the number of ADS-B equipped aircraft in range. In peak times, it can reach over 40–50 percent on average, with some aircraft experiencing prohibitively high loss rates of 80 percent or more.

***Message Collisions*** — Going further into details, message collisions seemed to have caused the recorded loss. With only a few aircraft, the loss rate is approximately 10 percent, rising to over 45 percent with 60 ADS-B senders. Considering this is not an unusual aircraft accumulation in many high-density airspaces around airports where hundreds of aircraft can be in communication range, this poses a significant problem. However, our simulations showed that the message rate of ADS-B alone could not be the root of the problem.

As mentioned before, it is not only ADS-B that is operating on the 1090MHz channel. In real-world environments, the interrogations and responses of Mode S and the related Mode A and C systems account for a large number of messages sent over the channel at any given time, more than 50 times the amount of ADS-B messages in our empirical samples. Mode A/C and S messages are sent by approximately 1.5 times as many aircraft as those that broadcast ADS-B. The observed loss of ADS-B messages is consistent with further simulations that we conducted to estimate the amount of collisions affecting ADS-B messages. The blue (dashed) line in Fig. 3c shows the results when taking into account all relevant ATC protocols, illustrating the severity of the problem with typical aircraft numbers. ADS-B was originally developed to cope with such high-density traffic, and it could indeed successfully achieve this if it were to use the 1090MHz frequency exclusively.

In the real world as it presents itself currently, ADS-B service is highly erratic when the number of aircraft in transmission range increases, particularly in high-density airspaces around airports during busy hours. These effects certainly need to be considered in receiver positioning and protocol development as they constitute a severe problem for the future deployment of ADS-B and other systems utilizing its data such as TCAS. Antenna design, interrogation rate management, and improved coordination between systems are examples of mitigating approaches that need to be examined as well as other previous work on 1090MHz channel capacity improvement [8].

## Further Insights

We identify the following typical effects that influence the deployment and usage of sensors and receivers in a network.

**Propagation model**: Our measurements verified that the standard log-distance path loss model fits the large-scale fading of line-of-sight communication of ADS-B systems well, while small-scale fading was log-normally distributed with standard deviation $\sigma = 1.15$.

**Doughnut effect**: There are noticeable "holes" in the reception quality of messages that are sent in close horizontal distance to a sensor with very high transmission power. This clipping effect can be seen in Fig. 3a, where the loss rate is higher in very close proximity (approximately 10-20km) to the receivers compared to further away.

**Antenna effects**: Aircraft equipped with ADS-B typically use two antennas for alternatingly transmitting messages, which can lead to differences in transmission characteristics such as RSSI values. Since there is no indicator on the antennas given, a filter would be needed to separate these, making the data analysis more complex.

**Duplicate messages**: There is some occurrence of duplicate messages in the data, caused by multipath effects. This is naturally stronger in mountainous areas and needs to be taken into account for protocol development and further processing of messages. On top of this, some current ADS-B transponders exhibit unspecified behavior, sending the same message a number of times (up to 12 or more in our data).

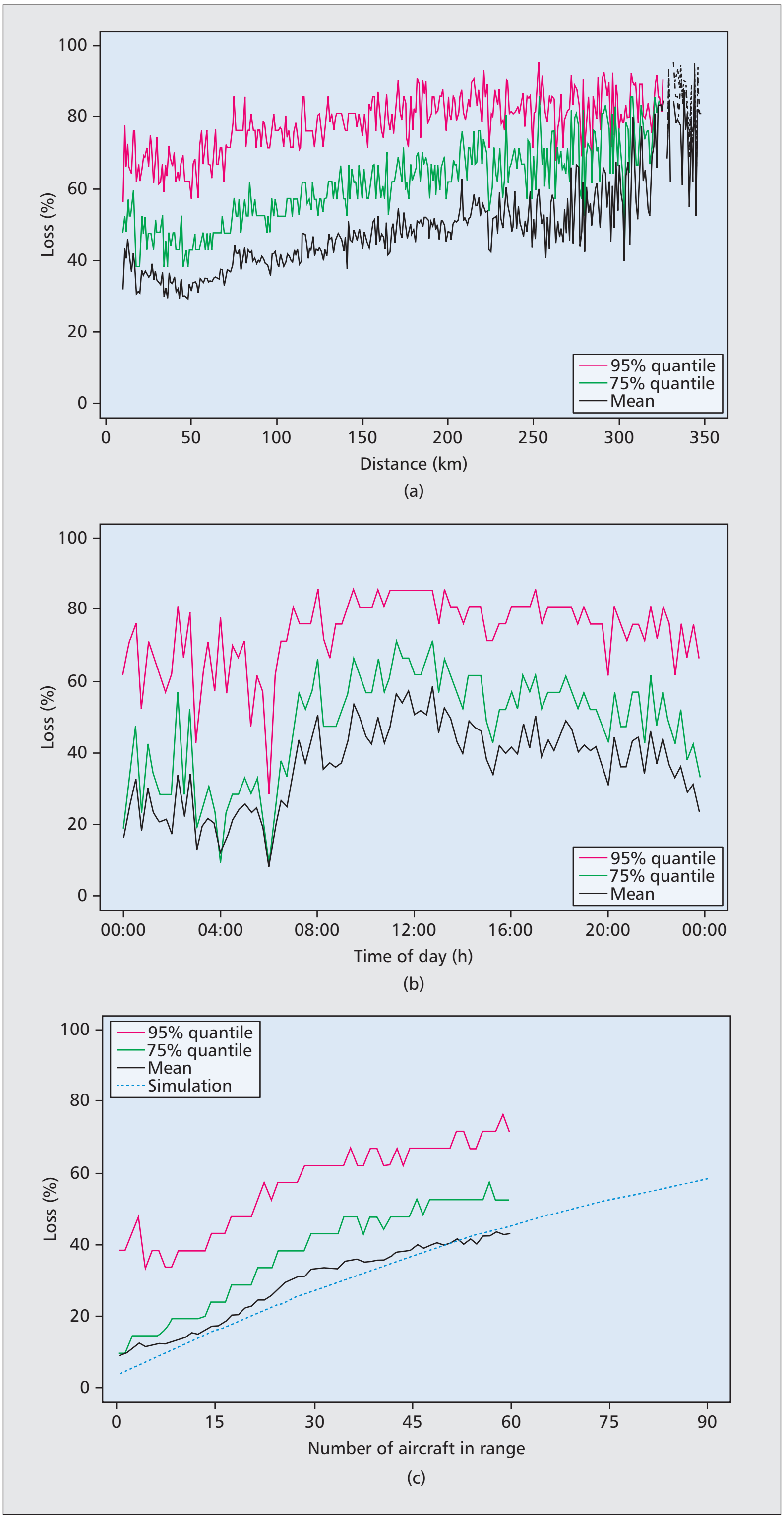


**Figure 3.** ADS-B message loss statistics: a) loss vs. distance; b) loss vs. time of day; and c) loss against number of ADS-B senders in close transmission range.

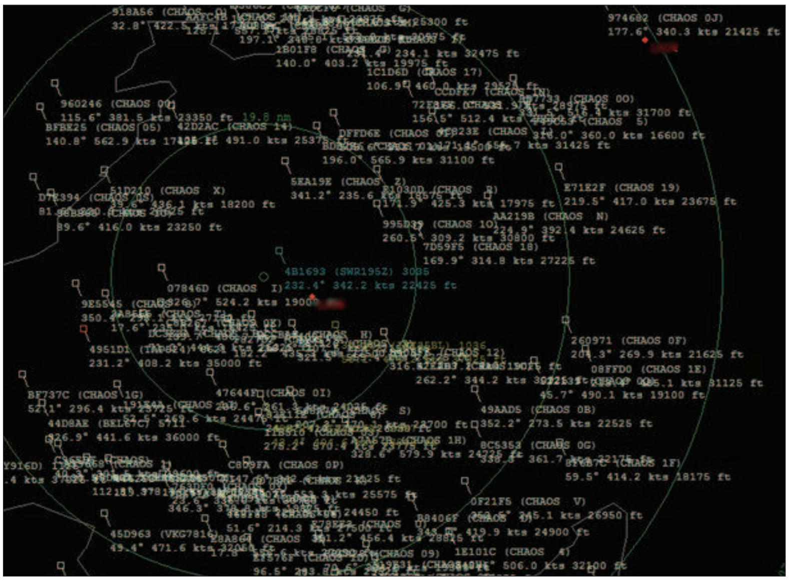


Figure 4. Example of a combined ghost aircraft flooding and injection attack, causing a denial of service on the receiver's end [10].

**Weather effects**: We found little effect of weather on RSSI (i.e. around 1dB decrease caused by rain and humidity, around 2dB for sun solar activity) and no effect on SNR. There was no conclusive effect on average loss and error rates.

## Security Considerations

Besides severe problems with message loss, another challenge for ADS-B that has recently been identified are security issues. For example, as seen on hacker conventions [9], ADS-B is highly susceptible to RF attacks, which generated a notable amount of media attention.[2] Just as high message loss on the 1090MHz frequency, adversarial action on the ADS-B data link may have a severe negative impact on collision avoidance and separation abilities of affected aircraft. These recent developments suggest that it is important to address those concerns as early as possible, as they pose a considerable problem for future widespread deployment of the protocol.

There are vulnerabilities in ADS-B that are inherent to the broadcast nature of unsecured RF communication. When the design assumptions for the ADS-B protocol were first discussed about two decades ago, the manipulation of RF communication was considered a possibility for only the most sophisticated and powerful adversaries. The required cost and engineering knowledge were seen as too prohibitive to consider further security mechanisms for the ADS-B protocol. With the advent of cheap and accessible software-defined radios as well as specialized receiver hardware for the reception of air traffic communication over the past few years, the threat model shifted considerably. Today, typical wireless attacks such as eavesdropping, jamming and modification, insertion and deletion of messages, are easily possible by anyone with widely available standard hardware and software, as recently illustrated in [5, 9, 10] among others. In the following, we give an overview of these attacks and their potential impact. Possible approaches to address these vulnerabilities have been discussed in [11].

### Vulnerabilities of the ADS-B Data Link

Any passive adversary can record and analyze the unencrypted ADS-B messages. However, an attacker that can actively interfere with ATC communication poses a much more severe threat to security than a merely passive one. From the findings in [10], we can assume that an attacker has full control over the wireless communication channel and is able to inject, delete, and modify any ADS-B message at will. A number of active attacks can be carried out with cheap, standard off-the-shelf hardware:

**Ground Station Flooding**: Continuous traditional jamming attacks on the 1090MHz channel would lead to high loss and message deletion in addition to naturally occurring collisions due to the random channel access of ADS-B and Mode S. This is a low difficulty attack, only constrained by the signal power of an adversary. It would force air traffic controllers to switch to older, lower precision surveillance techniques with potentially fatal consequences, especially in high density airspaces around major international airports.

**Ghost Aircraft Injection/Flooding**: It is possible to inject fake ADS-B messages claiming non-existing aircraft (so-called ghosts) onto the 1090MHz channel [5, 12]. Any legitimate ADS-B receiver would consider these fake messages as indistinguishable from real aircraft, leading to serious confusion for both pilots and air traffic control, particularly under poor signal and visibility conditions, when reliance on instruments is highest.

Besides a targeted, surgical injection attack that aims to be more subtle and not quickly detected, it is easily possible to flood ADS-B receivers with the injection of many aircraft at the same time. This may lead to a denial of service of a controller's airport and airspace surveillance systems. Without the support of other surveillance technologies, management may become impossible. Fig. 4 shows an exemplary implementation of a ghost aircraft injection and flooding attack on a given radar picture.

**Aircraft Disappearance**: Deleting all ADS-B messages sent by a particular aircraft would lead the aircraft to disappear completely from an ADS-B-based ATC application. The attack is more subtle and surgical than simple flooding, but similarly controllers have to rely on less precise surveillance systems such as PSR, defeating the original purpose of ADS-B. All attacks that require message deletion or modification are more complex to carry out with regard to timings. Still, by carefully positioning themselves, attack ranges of 100km or more are achievable with standard software-defined radio hardware.

**Virtual Trajectory Modification/False Alarm Attack:** This attack aims to modify the position and trajectory broadcast by a real aircraft. This can be achieved by both selectively jamming the actual messages at the ground sensor and replacing them with new ones, modified by the attacker. Alternatively, ADS-B messages can be modified directly on the air. If done subtly enough, the takeover would be hard to notice with less accurate PSR surveillance technologies

[2] *For example, http://www.forbes.com/sites/andygreenberg/2012/07/25/next-gen-air-traffic-control-vulnerable-to-hackers-spoofing-planes-out-of-thin-air/.*

and may lead to problematic situations for air traffic controllers.

In a more sophisticated version of the attack, ADS-B messages are modified to cause false alarms. ADS-B offers mechanisms to indicate emergencies or interferences such as aircraft hijacking, which may lead to serious consequences if abused.

**Aircraft Spoofing:** Every aircraft carries a 24-bit identifier assigned by the ICAO which can simply be changed with a combination of message deletion and injection attacks. Masquerading as a known or trusted aircraft may reduce propensity to cause red flags or alarms when an unexpected aircraft is detected through other means of surveillance.

## Future Perspectives for ADS-B and UAVs

Besides traditional aviation, modern unmanned aerial vehicles represent another area in which ADS-B will play a crucial role in the near future, specifically for SAA systems which are critical to collision avoidance. It has widely been touted as the future of UAV control, and a number of real-world tests have been conducted in the recent past.[3] Certification for a UAV requires the manufacturer to prove that its capabilities are at least as good as a manned counterpart; as of 2013, UAVs have been denied access to civil airspaces. Until now, FAA regulations have been highly prohibitive for normal airspaces, expecting SAA to work without cooperation by other aircraft, but this paradigm is shifting as well. There is much recent research being done on SAA systems using a cooperative approach with ADS-B, superseding traditional practices utilizing visual means [13]. According to industry reports, the FAA is consequently looking to formulate standards on using such electronic means for SAA by 2016,[4] making the issues discussed in this article even more pressing.

Recently, broad media exposure led the International Civil Aviation Organization (ICAO) to put the security of civil aviation on the agenda of the twelfth air navigation conference, identifying "cyber security as a high-level impediment to implementation that should be considered as part of the roadmap development process" [14] and creating a task force to help with the future coordination of the efforts from involved stakeholders. While these problems have been on the agenda of civil aviation stakeholders for some time now, the thematic constellation of UAV and ADS-B security will need to be assigned a higher priority, as for example Wesson and Humphreys [15] have also recently pointed out the severity of the situation. We believe these concerns will have to play a major role in academic and industrial research to enable safe certification of ADS-B-based SAA systems by 2020 and avoid further costly and embarrassing failures such as Germany's Euro Hawk recently. Euro Hawk, a spin-off of NATO's Global Hawk, was cancelled in May 2013 after 13 years of development due to ongoing regulatory and technical difficulties that made the project infeasible.

## Conclusion

In this article, we discussed the ADS-B protocol, the future standard of air traffic management. We introduced the development of ADS-B and examined if the historic assumptions could hold up when it will finally be rolled out until 2020. We argued that there are a number of problems that cause severe concerns for safety and security of future air traffic, particularly with the advent of Sense-and-Avoid-Systems for UAVs. Both issues, serious message loss caused by growing traffic on the 1090MHz channel and open security concerns due to the cheap and easy availability of software-defined radios, have severe implications for the final integration of ADS-B as a core part of the NextGen ATC system. Our findings strongly suggest that these issues will have to be addressed by the academic community and the ATC authorities as soon as possible, so the planned replacement of PSR/SSR with ADS-B will not be an illusion.

*Our findings strongly suggest that these issues will have to be addressed by the academic community and the ATC authorities as soon as possible, so the planned replacement of PSR/SSR with ADS-B will not be an illusion.*

### References

[1] RTCA Inc., "Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)," DO-242A (including Change 1), Dec. 2006.

[2] C. Rekkas and M. Rees, "Towards ADS-B implementation in Europe," *IEEE Tyrrhenian Int'l. Wksp. Digital Communications — Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*, , Sept. 2008, pp. 1–4.

[3] M. Schäfer *et al.*, "Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research," *ACM/IEEE Int'l. Conf. Information Processing in Sensor Networks (IPSN)*, Apr. 2014.

[4] RTCA Inc., "Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance — Broadcast (ADS-B) and Traffic Information Services — Broadcast (TIS-B)," DO-260B (with Corrigendum 1), Dec. 2011.

[5] D. McCallie, J. Butts, and R. Mills, "Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System," *Int'l. J. Critical Infrastructure Protection (IJCIP)*, vol. 4, no. 2, Aug. 2011, pp. 78–87.

[6] A. Smith *et al.*, "Methods to Provide System-wide ADS-B Back-Up, Validation and Security," *IEEE/AIAA Digital Avionics Systems Conference (DASC)*, Oct. 2006, pp. 1–7.

[7] L. Vidal, "ADS-B Out and In — Airbus Status," *ADS-B Taskforce — KOLKATA*, Apr. 2013.

[8] E. G. Piracci *et al.*, "1090 MHz Channel Capacity Improvement in the Air Traffic Control Context," *Int'l. J. Microwave and Wireless Technologies (IJMWT)*, vol. 1, July 2009, p. 193.

[9] A. Costin and A. Francillon, "Ghost in the Air (Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices," *Black Hat*, July 2012.

[10] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication," *Int'l. Conf. Applied Cryptography and Network Security (ACNS)*, Springer, June 2013, pp. 253–71.

[11] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ADS-B: State of the Art and Beyond," arXiv preprint arXiv:1307.3664, July 2013, available: http://arxiv.org/abs/1307.3664.

[12] L. Purton, H. Abbass, and S. Alam, "Identification of ADS-B System Vulnerabilities and Threats," *Australian Transport Research Forum (ATRF)*, Canberra, Australia, Sep. 2010, pp. 1–16.

[13] B. Stark, B. Stevenson, and Y. Chen, "ADS-B for Small Unmanned Aerial Systems : Case Study and Regulatory Practices," *IEEE Int'l Conf. Unmanned Aircraft Systems (ICUAS)*, May 2013, pp. 152–59.

[14] "Twelfth Air Navigation Conference," *ICAO*, Nov. 2012, pp. 1–4.

[15] K. Wesson and T. Humphreys, "Hacking Drones," *Scientific American*, vol. 309, no. 5, Oct. 2013, pp. 54–59.

[3] *For example by Sagetech: http://www.sagetechcorp.com/news/ottawa-flight-test-demonstrates-sense-and-avoid-capabilities-of-uavs.cfm or FLARM: http://flarm.com.*

[4] *http://www.ainonline.com/aviation-news/ain-air-transport-perspective/2013-07-22/faa-plans-unmanned-sense-and-avoid-rule-2016.*

## Biographies

Martin Strohmeier (martin.strohmeier@cs.ox.ac.uk) is a DPhil candidate and teaching assistant in the Department of Computer Science at the University of Oxford. His current research interests are mostly in the area of wireless network security, including next generation air traffic control and wireless sensor networks. Before coming to Oxford in 2012, he received his MSc degree from TU Kaiserslautern, Germany and also worked as visiting researcher at Lancaster University's InfoLab21 and Deutsche Lufthansa AG.

Matthias Schäfer (schaefer@cs.uni-kl.de) is a Ph.D. candidate in the Department of Computer Science at the University of Kaiserslautern, Germany, where he also received his M.Sc. degree in computer science in 2013. Between 2011 and 2013, he worked for the Information Technology and Cyberspace group of armasuisse, Switzerland and visited the Department of Computer Science of the University of Oxford, UK, as a visiting researcher.

Vincent Lenders (vincent.lenders@armasuisse.ch) has been working at armasuisse since 2008 where he is responsible for the Cyberspace and Information research program. Besides research, he has been deeply involved in the development of the cyber security concepts for the operational C4ISTAR systems of the Swiss Air Force. He earned his M.Sc and Ph.D. degree at ETH Zurich and was postdoctoral researcher at Princeton University. Since 2012, Vincent Lenders serves as the industrial director of the ZISC research center at ETH Zurich.

Ivan Martinovic (ivan.martinovic@cs.ox.ac.uk) is an Associate Professor at the Department of Computer Science, University of Oxford. His research interests are in the area of system security and wireless communication. Before coming to Oxford he was a postdoctoral researcher at the Security Research Lab, UC Berkeley and at the Secure Computing and Networking Centre, UC Irvine. He obtained his Ph.D. from TU Kaiserslautern and M.Sc. from TU Darmstadt, Germany.