On the Applicability of Satellite-Based Air Traffic Control Communication for Security

Martin Strohmeier, Daniel Moser, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic

Abstract

As air traffic control communication moves toward digital systems, there is an emerging trend toward supplementing or even fully substituting the traditional air-ground link in favor of communication between aircraft and satellites. In this article, we analyze coverage and security against wireless attacks of the novel satellite-based version of the Automatic Dependent Surveillance-Broadcast (ADS-B) technology. We compare it to the widely deployed terrestrial ADS-B system, which is known to be insecure and is inherently unable to provide coverage in some parts of the global airspace, such as oceans and polar regions. Our analysis shows that satellites can provide vast advantages in such non-surveillance areas. However, they are as fundamentally insecure as terrestrial ADS-B.

Introduction

Developed in the 1990s, the Automatic Dependent Surveillance-Broadcast (ADS-B) protocol forms the key part of the global NextGen airspace surveillance programs. ADS-B provides a wide range of benefits, from cost savings to improved situational awareness for pilots and controllers. To this end, it aims to improve the accuracy and update rates of aircraft positions during flight. This in turn leads to better handling by air traffic control (ATC) and the possibility to decrease separation minima between aircraft, a coveted prize for the increasingly congested airspace and airports around the world.

However, the security of this wireless technology was never considered during its design phase. For reasons of cost and compatibility, ADS-B was developed based on existing 1970s technology and was overtaken by technological developments in the late 2000s. Novel flexible software-defined radio (SDR) techniques enabled hackers and academic researchers to prove that the unencrypted ADS-B communication between aircraft and ground stations can easily be received and manipulated, leading to potentially severe impact on the business and safety operations of airports and airlines [1].

While ADS-B has been mandated from 2020 in Europe and the United States, a large proportion of affected aircraft and air navigation service providers (ANSPs) have not yet been equipped with the necessary hardware, making delays to the mandate look increasingly likely. In this climate, several entities have been working on extending the ground-based system to low Earth orbit (LEO) satellites.

This approach, dubbed space-based or satellite-based ADS-B (SADS-B), has quickly gained traction; in busy airspace it could provide improved operational efficiency and reduction of delays if primary radar sources fail.

One main selling point for SADS-B is its potential to bring surveillance to oceans and polar regions. Tracking aircraft in remote corners of the Earth became a renewed priority for aviation authorities due to the unsolved disappearance of Malaysian flight MH370. The combination of compulsory ADS-B transponder usage and satellite-supported ADS-B receivers would enable unprecedented coverage around the globe, ensuring that the whereabouts of airliners and larger civil aircraft — with active transponders — would always be known.

Some in the aviation community assume that SADS-B solves the known security issues surrounding ADS-B installations in the National Airspace System [2]. Executives of Aireon, the Canadian provider of one of the underlying satellite-based infrastructures, argue that it is impossible to attack SADS-B using the wireless medium (i.e., receivers in space are immune to injection or jamming attacks).[1]

To date, no security analysis of SADS-B has been undertaken. We make the following related contributions in this work:

- Based on current real-world assumptions, we compare the potential coverage of ground- and satellite-based ADS-B, and discuss the impact on security.
- We provide a first security analysis of space-based ADS-B receiver systems, showing that they are fundamentally vulnerable against both passive and active attacks, and describe the necessary theoretical underpinnings.
- We compare the costs for practical real-world attacks against both space- and ground-based ADS-B receivers, illustrating their feasibility for different adversaries.

Background

Figure 1 illustrates the traditional terrestrial ADS-B model (TADS-B). Aircraft communicate directly with ground receivers on a line-of-sight (LoS) basis (red arrows), following free-space path loss (FSPL) propagation [4].

The authors analyze coverage and security against wireless attacks of the novel satellite-based version of the Automatic Dependent Surveillance-Broadcast (ADS-B) technology. They compare it to the widely deployed terrestrial ADS-B system, which is known to be insecure and is inherently unable to provide coverage in some parts of the global airspace, such as oceans or polar regions.

[1] Aireon's CTO explains: "We're 485 miles up in space, so it's not like someone is going to be perturbing the signal. What they could perturb is the GPS signal, not the ADS-B signal." [3].

Martin Strohmeier and Ivan Martinovic are with the University of Oxford; Martin Strohmeier is also with armasuisse; Daniel Moser is with ETH Zurich and armasuisse; Matthias Schäfer is with the University of Kaiserslautern; Vincent Lenders is with armasuisse.

Digital Object Identifier: 10.1109/MCOM.001.1900037

Due to the LOS characteristics, ADS-B cannot be received terrestrially beyond the radio horizon, which is typically 400-500km for aircraft in the en-route airspace (an altitude of ca. 10km). Beyond this physical restriction, which makes comprehensive oceanic surveillance impossible, there are further non-surveillance territories caused by a lack of ground receivers in the area.

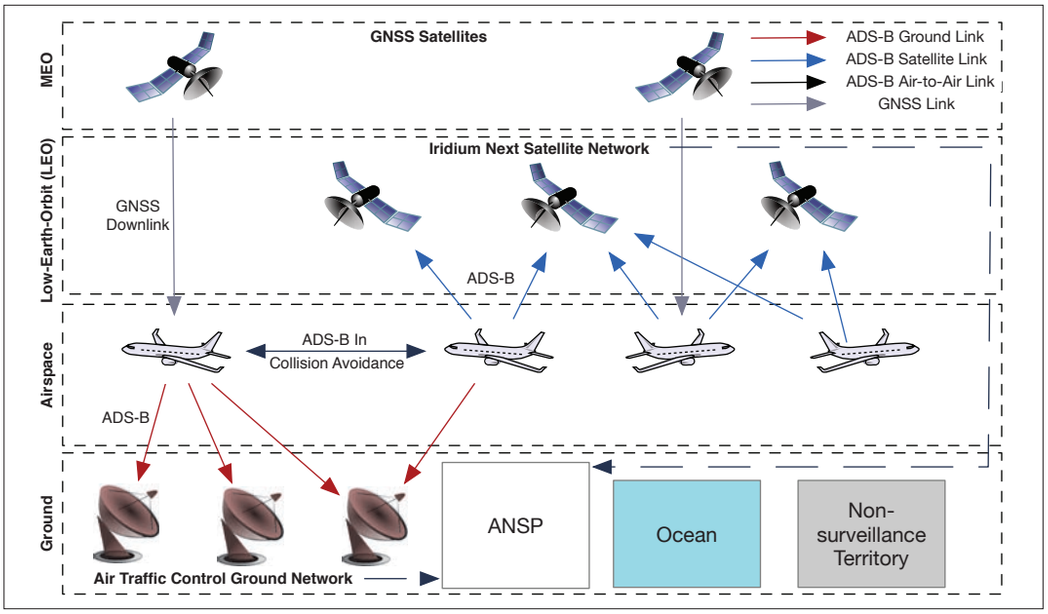

Figure 1. Overview of the ADS-B ecosystem.

There are two data links available (Table 1). The Universal Access Transceiver (UAT) link operates on the 978 MHz frequency and has been developed for use with ADS-B. In practice, it is only used by general aviation aircraft in North America and below an altitude of 18,000 ft. The second option is the 1090 MHz Extended Squitter (1090ES) data link, which is based on legacy secondary surveillance radar technology developed in the 1970s [4]. We focus on 1090ES in this work, as it is set to become the global standard across all altitudes and aircraft types.

Some of the content broadcast via ADS-B is obtained using satellites even in the terrestrial model. In particular, an aircraft's own position is measured via global navigation satellite systems (GNSSs) stationed in medium Earth orbit (MEO) at an altitude of 19,000–23,000 km. The data is broadcast at 2 Hz, providing an update rate sufficient for busy airspaces and approach control, even in high-loss environments.

Terrestrial ADS-B System Model

Due to the LoS characteristics, ADS-B cannot be received terrestrially beyond the radio horizon, which is typically 400–500 km for aircraft in the en route airspace (an altitude of approximately 10 km). Beyond this physical restriction, which makes comprehensive oceanic surveillance impossible, there are further non-surveillance territories caused by a lack of ground receivers in the area. Reasons include delays in development in some airspaces and the high cost of uninterrupted surveillance over large uninhabited areas.

Some of these issues can be overcome using cheap crowdsourced ADS-B receivers, which help in increasing the global coverage of the terrestrial ADS-B system toward the theoretical maximum.

Space-Based ADS-B System Model

While not originally specified for reception in space, the high transmission power of transponder-equipped aircraft allows for long ranges.

	1090ES	UAT	SADS-B
Frequency	1090 MHz	978 MHz	1090 MHz
Data rate	1 Mb/s	1 Mb/s	1 Mb/s
Max. effective range	ca. 500 km	ca. 300 km	3250 km
Receiver cost	Low	Low	High
Update rate	0.5–1 s	0.5–1 s	8 s (target)

Table 1. Comparison of ADS-B link options.

Aireon's SADS-B receiver implementation uses the Iridium satellite constellation. The ADS-B receivers are fitted as a payload to the new Iridium NEXT satellites that are deployed as a replacement for the aging Iridium fleet. The constellation consists of 66 active satellites in a total of 6 North-South orbits offset by 60° each. Each satellite keeps a direct link with its neighbors in the same and adjacent orbits. The average altitude of the active satellites is 780 km above ground, while a total of 9 satellites are kept at reserve orbits at higher altitude.

While the high altitude provides a privileged vantage point for Aireon's receivers, the inherent challenges (notably distance and channel utilization) of SADS-B reduce the effective update rate for the aircraft positions, which is expected to be 8 s for the 95th percentile [5]. Thus, SADS-B's main target is to provide situational awareness and decreased separation between aircraft for low-density en route airspaces over oceanic or unpopulated areas, instead of surveillance for busy terminal areas.

Coverage Analysis

We compare the coverage possible by TADS-B with the newest available data from Aireon's SADS-B network powered by Iridium. We first analyze the global coverage in 2D, before taking a look at how aircraft's altitudes influence reception on the ground and in space. Finally, we discuss processing and utilization issues arising from the large-scale coverage of the satellite system.

Horizontal Coverage

The comparison of the possible 2D coverage quantifies the natural advantage of satellite-based systems. As only 29 percent of the 510.1 million km^2 surface area of the Earth is covered by land, we cannot expect to cover some large areas purely with ground-based receivers (Fig. 2a).

Terrestrial ADS-B: We calculate the maximum Earth coverage for TADS-B, based on the available land mass, to place an ADS-B receiver. This can be regarded as an upper bound, as it is not possible to place ADS-B receivers on every piece of existing land mass, in particular in areas with limited infrastructure such as mountain ranges or the polar regions.

Figure 2a illustrates a buffer zone that is drawn as a parallel line 200 nm from any land mass, a typical radius found for the top ADS-B receivers within the OpenSky Network, a crowdsourced receiver network available to researchers (http://opensky-network.org).

We calculate that approximately 274 million km^2, or 53.7 percent of Earth's surface area, could theoretically be covered. This leaves a lower bound of almost half of the global airspace where aircraft cannot be tracked. As most countries outside Europe and North America have been slow to adopt ADS-B, this non-surveillance area is currently far greater in practice. Similar restrictions also apply to other complementary surveillance and radar technologies dependent on LoS communication.

Space-Based ADS-B: Figure 2b illustrates coverage of the Iridium NEXT constellation, enabling surveillance for the remaining 46.3 percent of Earth's surface. The coverage regions of neighboring satellites overlap, with the overlap increasing with distance from the equator. At the polar regions, consistently more than three satellite reception ranges overlap; closer to the equator, there are areas covered by only a single satellite.

Naturally, most daily flights never cross into regions without ground coverage; to quantify the added value of SADS-B beyond theoretical calculation, we look at the number of flights out of terrestrial reach.

To get a realistic estimate of this number, we analyzed data from Flightradar24 (http://flightradar24.com), which operates the most extensive global network of ground ADS-B receivers, over 20,000 as of April 2019. We took a snapshot of the global flight traffic every 6 hours over a 30-day period and compared the number of tracked flights with those that were previously tracked (i.e., after take-off) but listed as out of surveillance range at the time of the snapshot.

The data shows that on average 11.1 percent (min: 6.6 percent, max: 14.4 percent, std: 2.3 percent) of transponder-equipped aircraft are not within range of ground receivers. This illustrates that the real-world coverage advantage of SADS-B is below the physical improvement over TADS-B.

Vertical Range

LEO satellites require sufficiently high-powered ADS-B signals sent by the aircraft. In comparison to terrestrial receivers, which largely require LoS (i.e., a good placement away from overshadowing buildings) for reception up to the radio horizon and which face no practical vertical constraint, this impacts the efficacy of SADS-B in practice. We analyze the two main factors that influence the reception of an ADS-B transponder-equipped aircraft, antenna placement and flight level, and quantify their impact on the practical vertical range of SADS-B.

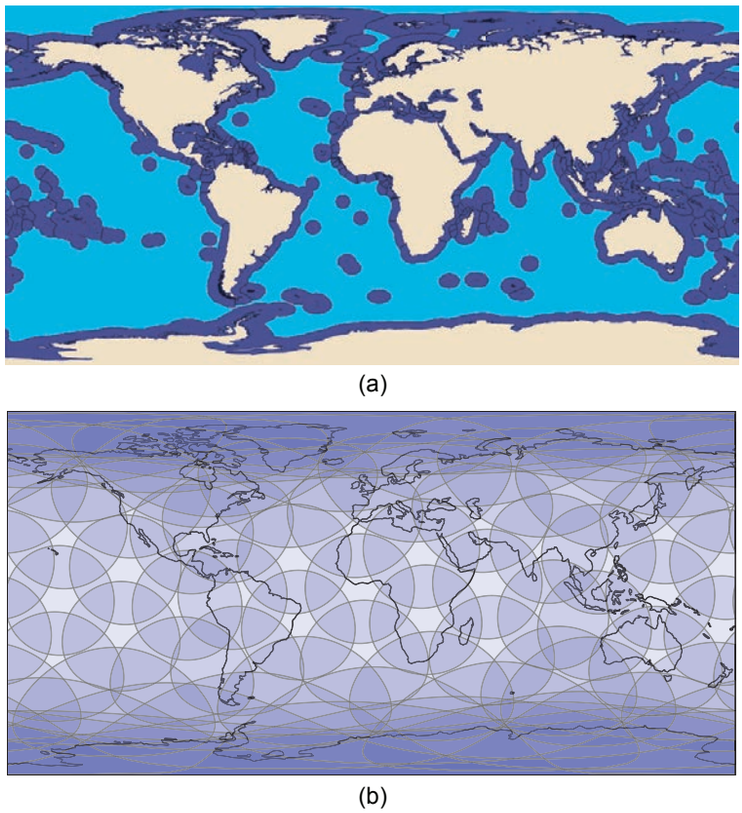

Figure 2. a) Map with 200 nm buffer zones around all land mass, approximating the maximum ground ADS-B coverage; b) Iridium's theoretical coverage on a reported range of approximately 3000 km.

Flight Level: Aireon's design specifications assumed that for aircraft in lower altitudes, the likelihood of reception drops significantly. Early tests of the deployed system have had more optimistic results and showed the possibility of at least some lower altitude reception under good conditions [6]. From a regulatory standpoint, however, the update rates likely remain insufficient for operational surveillance at these altitudes.

We analyze the impact of this issue by analyzing unfiltered snapshots of ADS-B traffic provided by the OpenSky Network every six hours over a 30-day period and examining the average distribution of aircraft across different altitudes (so-called flight levels, or FLs, given in 100 ft distances). Across the 593,329 flights observed over this time frame, Table 2 shows that at the time of the snapshots, 199,475 or 33.62 percent were below FL200 and 167896 or 28.3 percent below FL150 (i.e., the ranges where reception with SADS-B becomes more patchy).

Antenna Diversity: Existing standards for 1090ES mandate that all aircraft with a maximum takeoff weight ≥ 5700 kg plus smaller aircraft capable of a maximum cruising speed ≥ 463 km/h and/or cruising altitudes of ≥ 15,000 ft, carry two

An effective attack requires knowledge of the receiver positions. The positions of all Iridium Next satellites are public and can be calculated in advance. Thus, getting this information is easier than for the ground case, where all involved receiver positions must be obtained through intelligence or observations; missing one could give away the attack.

antennae [7]. One is placed on the bottom and one on top of the fuselage, increasing diversity and robustness. If only one antenna is mounted on the aircraft, it is mounted at the bottom to optimally support terrestrial ATC receivers.

However, SADS-B works best for the top-mounted antennae on larger aircraft. Based on the above defined standards, we can estimate that 96.8 percent of all ADS-B-equipped aircraft have a top-mounted antenna, and 99.4 percent of all observed flights are conducted with antenna diversity (AD; see Table 2).

This can be considered as an upper bound for transponder-equipped flights with consistent SADS-B reception. Smaller general aviation aircraft can use significantly less power compared to larger airliners, which must emit a peak transmission power of at least 125 W (21 dBW) with many reaching up to 250 W (24 dBW). However, the latest experiments with a Cessna show at least some bottom-only reception from satellites at advantageous angles [6].

Channel Utilization

Compared to terrestrial reception, SADS-B receivers cover a much larger area with more concurrent aircraft and thus must process more messages. As ADS-B does not implement a medium access control approach, this causes severe problems for effective channel utilization. The 1090 MHz frequency in particular has suffered from heavy use by several different ATC technologies, most notably the traditional secondary surveillance radar (SSR). Even for more localized ground-based receivers, these capacity restrictions result in interference and message loss of 50–90 percent in busy airspaces with several hundred aircraft [4].

Existing studies of the satellite footprint indicate significant interference by both desired signals and signals from non-aviation technologies operating on the same frequency. In many simulations based on these assumptions, there was a 10 percent chance of not receiving any position messages from an aircraft for ≥ 5 minutes [8].

Security Threat Analysis

We now discuss realistic security threats to SADS-B, how they compare to TADS-B, and whether assumptions of increased protection exclusively through receiver placement in space are accurate.

General Security in ADS-B

Much attention has been paid to ADS-B security. Motivated by initial findings from the hacker community, a significant academic body of research has evaluated the vulnerabilities of the technology and the possible consequences, ranging from ghost aircraft on radar screens to denial-of-service attacks (see [9] for an extended overview).

This attention has forced authorities to put the issue on their agenda, as evidenced by a recent report from the U.S. Government Accountability Office. The report pressed the urgency of the matter considering the mandatory adoption of ADS-B in 2020 for military aircraft as well [10].

The inherent vulnerabilities of ATC protocols do not come as a surprise to experts, considering the lack of authentication, integrity, and confidentiality. However, with the wide accessibility of SDRs and downloadable software, active attacks have become realistic.

Flight level	Flights	Ratio (%)	Flights w/ AD	Ratio (%)
< FL20	44057	11.19	42730	96.99
< FL50	86433	14.57	83860	97.02
< FL100	132680	22.36	129450	97.57
< FL150	167896	28.3	164317	97.87
< FL200	199475	33.62	195896	98.21
> FL200	393854	66.38	393854	100
Sum	593329	100	589750	99.4

Table 2. Analysis of satellite tracking based on aircraft altitude and antenna diversity (AD).

The authors in [1, 11] have shown the practicability of SDR-based attacks, from jamming and signal manipulation to message injection. They derive requirements regarding the attacker's placement and signal strength for successful attacks against ADS-B ground receivers. We extend this analysis for the satellite case.

Security Analysis of SADS-B

Fundamentally, there is no additional security in SADS-B as there are no modifications to the protocol, and satellites receive the same unauthenticated signals as ground receivers. Aireon encrypts their payload for transportation from satellite to their ground network, from where it is distributed to the ANSPs [3]. Assuming no flaw in the proprietary process, this protects the payload against injection and modification attacks (although not against the threat of localized jamming).

Crucially, however, encrypting happens only after reception of the ADS-B messages at the satellite. Thus, all the same attack types demonstrated for ground receivers are possible with SADS-B, too, although their application in practice is more difficult.

Satellite Position Knowledge: An effective attack requires knowledge of the receiver positions. The positions of all Iridium Next satellites are public and can be calculated in advance. Thus, getting this information is easier than for the ground case, where all involved receiver positions must be obtained through intelligence or observations; missing one could give away the attack.

Impact of Relative Attacker Positions: The attacker position has a crucial impact on the feasibility of more sophisticated attacks such as jamming or signal manipulation [1]. Figure 3 illustrates the relative positions between attacker *A*, airplane *P*, and receiver *R*, for both the ground and satellite cases.

This analytical approach shows that these more complex attacks, which require tight reaction times, are truly more difficult in the satellite case. As one cannot easily reach a relative position between aircraft and satellite, the angle α_s becomes less favorable compared to α_g in the ground case. In fact, as reactive attacks require the attacker to receive the legitimate signal prior to transmitting their own interference signal, no reactive attack on satellites can be launched

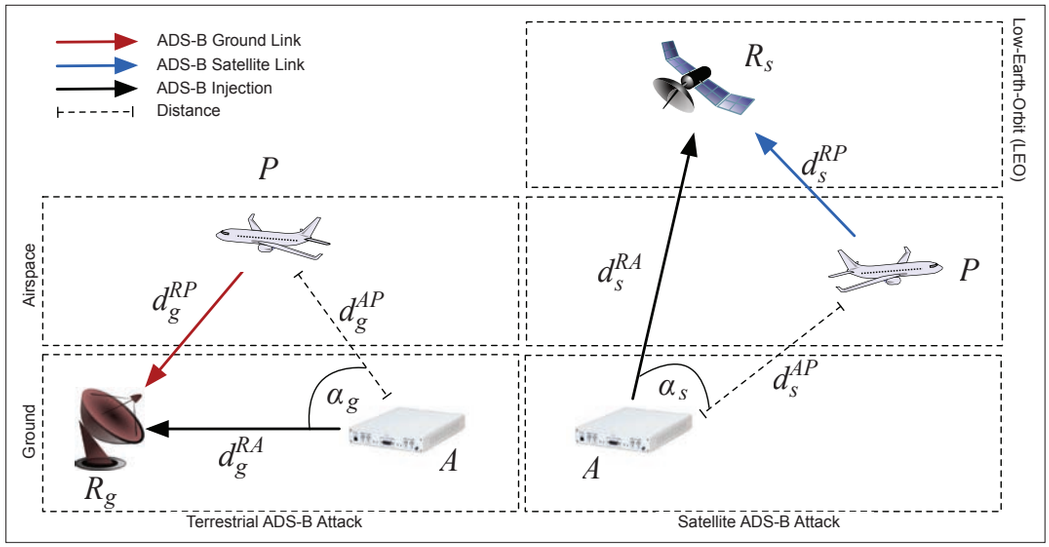

Figure 3. Illustration of attacks on terrestrial and satellite ADS-B.

from the ground — the attacker's signal would not arrive in time. However, message injections, which form the basis for the simplest and most likely attack vectors, are not impacted by the relative position of the attacker and thus face no additional constraints in SADS-B [1].

Theoretical Considerations for Message Injections: The simplified requirement for a message injection attack on a receiver R is defined as follows: $rx_{AR} > S_R$, where rx_{AR} represents the received power at R emitted by the attacker A and S_R the receiver sensitivity (i.e., the signal strength to correctly demodulate the signal). Hence, the determining factor is the transmission power expended by the attacker.

Thus, with correctly modulated signals in the right message format, it is possible to conduct an attack independent of the receiver's position. A receiver placement in space requires slightly more expensive and sophisticated hardware; we now describe the exact additional requirements.

Comparison of Resources for Successful Attacks

While it is indeed more difficult in terms of hardware resources to attack the satellites powering SADS-B, we show that the difference is small, and remains within the realm of non-institutional attackers. Table 3 lists the capability requirements.

Attack Requirements for TADS-B: The rise of SDR technology has lowered the requirements for attacks on wireless technologies significantly over the past decade.

Hardware: Beyond a standard portable computer device (e.g., a Raspberry Pi or a laptop), three hardware components are necessary to send properly modulated ADS-B messages on the 1090 MHz channel with sufficient power: SDR, antenna, and amplifier. The SDR can range from top-end USRP devices ($2000) to affordable HackRF versions ($290), both with integrated amplifiers, down to easily converted USB-to-VGA cables for $10. Capable antennae are available from $20.

Transmission Power: Under practical assumptions for the target's sensitivity of S_R = −91 dBm and its antenna gain of rx_{gain} = 11dBi (exemplified by a Thales AX680 ground station), the attacker can achieve the injection attack with the HackRF's full sending power of tx_{power} = 10 dBm and an antenna gain of tx_{gain} = 8dBi. Given LoS, the communication can theoretically be received from about d_g^{RA} = 22 km away without additional hardware.

Software: Whereas software allowing reception of ADS-B signals with SDRs has been available since 2012, and it was feasible for technically skilled adversaries to adapt this software to also enable transmission, several full software suites have appeared on public online repositories over the past 24 months. Using, for example, WALB [12], it is now possible for even low-skilled adversaries to execute an injection attack using the HackRF platform.

Attack Requirements for SADS-B: Similarly, we derive the minimum requirements for an injection attack against an Iridium Next SADS-B receiver. Besides light modifications to the hardware, an attack involves exploiting the public knowledge about satellite positions and following the moving angle of the target satellite's LoS.

Hardware: For message injections, the same setup can be used as with TADS-B. We add a sufficiently powerful directional antenna and amplifier to increase the transmission strength to reach the satellite receivers (Table 3).

Transmission Power: Assuming a distance between ground and target satellite of d_s^{RA} = 780 km, the attacker needs to overcome a path loss of 151 dB and additional losses (e.g., cable, connectors) of conservatively estimated about 5 dB. With real-world values for the target's sensitivity of S_R = −95 dBm and an antenna gain of rx_{gain} = 8 dBi, the attacker can inject messages with $tx_{power} \geq 45$ dBm and an antenna gain of $tx_{gain} \geq 8$ dBi.

To achieve this, the attacker needs to connect their low-cost, low-power device to a power amplifier providing an output power of up to ≥ 100 W (or 50 dBm). Such amplifiers sell on the used market from about $1000 alongside professional directional antennae with gains of up to 16 dBi.

The increased power requirements make the setup both more expensive and easier to detect (visually or by monitoring the spectrum). How-

Whereas software allowing reception of ADS-B signals with SDRs has been available since 2012, and it was feasible for technically skilled adversaries to adapt this software to also enable transmission, several full software suites have appeared on public online repositories over the past 24 months.

Directed injections against only a single satellite cannot be detected using TDoA; they require plausibility checks and remain a problem in areas near the equator not covered by multiple satellites. Future work should examine the applicability of other physical-layer characteristics such as Doppler shift, angle of arrival, or signal strength, which have been proposed for the terrestrial case.

ever, the cost remains within reach of non-state actors. Furthermore, the wide LoS ranges of satellites provide a significant advantage to an attacker compared to terrestrial targets; they can launch an attack from up to 3000 km away (i.e., a neighboring country or uninhabited areas), and thus evade detection and physical access by state forces.

Software: As there are no changes on the physical and protocol layers with SADS-B, the same software can be used as in the terrestrial case.

Countermeasures

The inherent vulnerabilities of ADS-B and other unsecured ATC technologies inspired recent research into potential countermeasures. They can broadly be categorized into approaches that change the underlying technology and those that work transparently alongside the existing system [9]. As time-consuming development and certification cycles are required for fundamental changes in an industry with lead times of > 15 years, a shorter-term focus remains on *physical-layer countermeasures*. The most popular involves the independent verification of aircraft signals using the time differences of arrival (TDoAs) between multiple receivers, which is also the basis of the multilateration technique. TDoA has low bandwidth requirements, feasible for limited satellite connections compared to other physical characteristics (e.g., frequency).

With the overlapping coverage provided by SADS-B (Fig. 2b), it is infeasible to localize aircraft in most areas using TDoA, as this requires three or more satellites to receive a single message and depends on optimal geometric receiver constellations. With only two receivers it is possible to use statistical or machine learning methods (see [9] for further readings) to verify the veracity of an aircraft's position independently of the claim in the ADS-B message itself, thereby detecting data injections (or non-malicious issues).

Aireon, developers of the most advanced SADS-B, are investigating such options, including an "Independent Position Validation Solution" scheduled for 2020 [5]. With 80 percent of the Earth covered by at least two satellites, using TDoA could provide a powerful addition to the fragile ADS-B security ecosystem.

Attacks against Satellite TDoA Verification: While physical-layer verification cannot substitute cryptography-based security by design, it raises the attack difficulty significantly. To circumvent TDoA-based verification, an attacker needs high-precision transmission capabilities [13]:

- **Transmission chains:** The attacker needs to deploy multiple transmission chains.
- **Timing:** Low-cost SDRs such as the HackRF are not capable of transmitting precisely timed signals, requiring more advanced SDR platforms with nanosecond-precise transmission (e.g., Ettus USRP with GPSDO).
- **Aim:** The attacker needs highly directed antennae to target each visible satellite individually.
- **Track:** Iridium satellites travel at about 27,000 km/h and are visible for < 10 min, requiring the attacker to track their trajectory and transmit the signals to the correct satellite.

	TADS-B	SADS-B
Distance	0-20 km	ca. 780 km
Software	Free (e.g., WALB [12])	Free (e.g., WALB [12])
Transmitter	HackRF ($290)	HackRF ($290)
Antenna gain	8 dBi ($20)	16 dBi (ca. $200)
Amplifier	None/integrated	100 W (ca. $1000)

Table 3. ADS-B injection attack requirements.

Analysis: Considering the feasibility of attacking satellites, independent physical-layer verification is a promising countermeasure, as previously suggested by security researchers [9, 11, 13].

At this early stage of SADS-B, there are, however, open questions about its versatility, which will require further analysis after full deployment. For example, usable TDoA opportunities (i.e., signals seen by two or more satellites) are available only for about 6 percent of all received messages [5]. Combined with update rates of up to 8 s [6], attacks might not be detected for several minutes in the worst case.

Second, validating an aircraft's altitude remains more difficult and less accurate using TDoA, both from ground or space. Spoofing this altitude could prove highly problematic for ATC and collision avoidance.

Lastly, directed injections against only a single satellite cannot be detected using TDoA; they require plausibility checks and remain a problem in areas near the equator not covered by multiple satellites (Fig. 2b). Future work should examine the applicability of other physical-layer characteristics such as Doppler shift, angle of arrival, or signal strength, which have been proposed for the terrestrial case [9, 14].

Discussion

While SADS-B's focus is on surveillance for en route rather than terminal airspaces, busy areas near airports are where potential attacks are most disruptive and effective. Combined with its lower update rates, this severely degrades SADS-B's utility as a redundant technology in terms of security.

Other Satellite ADS-B Technologies

While Aireon runs the most advanced deployment, competing satellite services exist. The ADS-B Link Augmentation System (ALAS) [15] has been operational since 2010 and uses the LEO satellite constellation Globalstar. It promises to fix "the open and unsecured nature of ADS-B signals."

According to the developer, bidirectional IP-based satellite communication between aircraft and ground [15] enables encryption and protection against spoofing, intrusion, and jamming. ALAS has not enjoyed significant momentum, though, as it is not a standardized technology and requires aircraft to be fitted with costly new avionics [15]).

This contrasts with Aireon's SADS-B, which requires no modifications to the existing ADS-B environment. Indeed, other operators are entering the market with miniaturized CubeSat satellites, seeking to provide global coverage and update rates below 15 min. While it is too early to

closely scrutinize these systems, their fundamental characteristics and security issues are analogous to the implementation discussed in this work.

Wireless Link Monoculture

Due to the satellite model's attractiveness, there is a trend in aviation to forego new ground infrastructure and move in-flight entertainment (IFE) and communication, navigation, and surveillance (CNS) systems into space.

However, the phase-out of traditional air-ground links creates operational issues. As the three CNS functions become more interdependent and rely on some of the same satellite systems, safety-enhancing technological redundancy could decrease. Where independence between the navigation and surveillance functions gets reduced by the growing use of GNSS instead of terrestrial technologies, we risk a wireless link monoculture, which may be subject to easier interference.

Conclusion

There is a strong trend toward satellite-augmented communication systems in aviation, which offer several advantages over traditional terrestrial infrastructure: global coverage, homogeneous infrastructure deployment, and attractive service models. We have analyzed some of these benefits, along with the notable security issues of the involved legacy protocols.

SADS-B is poised to become an effective additional surveillance layer for the en route airspace, in particular in remote areas, but not a solution to all of ADS-B's existing issues. It will facilitate search and rescue missions and provide backup to failing primary radar infrastructures. However, in busy airspaces and outside en route areas, it will coexist with its ground-based counterpart to maintain sufficient low-altitude coverage and update rates.

The widely debated security problems of ADS-B remain, as they are caused by the inherent lack of encryption in the technology, a problem not solved by moving receivers into space. Indeed, the attack surface of satellites is as global as their increased coverage abilities. On the other hand, the added layer of receivers offers new opportunities for physical-layer verification, which, if implemented thoughtfully, may offset some of these concerns.

References

[1] 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*, 2013, pp. 253–71.

[2] C. Wargo *et al.*, "Ubiquitous Surveillance Notional Architecture for System-Wide DAA Capabilities in the NAS," *IEEE Aerospace Conf.*, 2018.

[3] T. Risen, "Tracking Airliners From Space," *Aerospace America*, July 2017; https://aerospaceamerica. aiaa.org/departments/tracking-airliners-from-space/, accessed 1 Apr. 2019.

[4] M. Strohmeier *et al.*, "Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B," *IEEE Commun. Mag.*, vol. 52, no. 5, May 2014, pp. 111–18.

[5] J. Dolan and M. Garcia, "Aireon Independent Validation of Aircraft Position via Space-Based ADS-B," *Int'l. Symp. Enhanced Solutions for Aircraft and Vehicle Surveillance Applications*, 2018.

[6] M. Garcia *et al.*, "A Compilation of Measured ADS–B Performance Characteristics from Aieron's On-Orbit Test Program," *Int'l. Symp. Enhanced Solutions for Aircraft and Vehicle Surveillance Applications*, 2018.

[7] *International Standards and Recommended Practices, Annex 10: Aeronautical Telecommunications*, 4th ed., ICAO, 2007, Volume IV: Surveillance and Collision Avoidance Systems.

[8] ITU-R, "Reception of Automatic Dependent Surveillance Broadcast Via Satellite and Compatibility Studies with Incumbent Systems in the Frequency Band 1,087.7–1,092.3 MHz," tech. rep. ITU-R M.2413-0, 2017.

[9] M. Strohmeier *et al.*, "On Perception and Reality in Wireless Air Traffic Communication Security," *IEEE Trans. Intelligent Transportation Systems*, vol. 18, no. 6, 2017, pp. 1338–57.

[10] J. Kirschbaum, "Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology that Tracks Military Aircraft," U.S. Government Accountability Office, tech. rep. GAO-18-177, Jan. 2018.

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

[12] crescentvenus, "Wireless Attack Launch Box (WALB)," 2018; https://github.com/crescentvenus/WALB, accessed 1 Apr. 2019.

[13] D. Moser *et al.*, "Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures," *22nd Annual Int'l. Conf. Mobile Computing and Networking*, 2016, pp. 375–86.

[14] A. Tart and T. Trump, "Addressing Security Issues in ADS-B with Robust Two Dimensional Generalized Sidelobe Canceller," *22nd Int'l. Conf. Digital Signal Processing*, 2017.

[15] C. T. Howell *et al.*, "The Use of a Satellite Communications System for Command and Control of the National Aeronautics and Space Administration Surrogate Unmanned Aerial System Research Aircraft," *Ass'n. for Unmanned Vehicle Systems Int'l. Xponential Conf.*, 2017.

Biographies

Martin Strohmeier (martin.strohmeier@cs.ox.ac.uk) is a junior research fellow at the University of Oxford and a scientific project manager at the Cyber-Defence Campus in Switzerland. Before coming to Oxford for his Ph.D., he received his M.Sc. from TU Kaiserslautern, Germany, and worked as a researcher at Lancaster University's InfoLab21 and Lufthansa.

Daniel Moser is a Ph.D. student at the Cyber-Defence Campus and the Department of Computer Science at ETH Zurich, Switzerland. His thesis topic covers different aspects of security and privacy of aircraft communication systems. He obtained his BSc and M.Sc. degrees in computer science from the University of Berne, Switzerland.

Matthias Schäfer is a lecturer and researcher at the distributed computer systems lab (DISCO) at the University of Kaiserslautern, Germany. Until 2018, he was a Ph.D. student supervised by Prof. Dr.-Ing. Jens B. Schmitt. Before that, he worked at armasuisse S+T and visited the University of Oxford in 2012. He is also a co-founder and board member of the OpenSky Network association and managing director of SeRo Systems GmbH.

Vincent Lenders is head of the Cyber-Defence Campus at armasuisse, Switzerland. He received his M.Sc. and Ph.D. degrees in electrical engineering and information technology from ETH Zurich. He was a postdoctoral research fellow at Princeton University. He is a co-founder and on the board of the OpenSky Network and Electrosense associations.

Ivan Martinovic is a professor in the Department of Computer Science, University of Oxford. Previously, he was a post-doctoral researcher at the Security Research Lab, University of California (UC) Berkeley and the Secure Computing and Networking Centre, UC Irvine. He obtained his Ph.D. from TU Kaiserslautern and his M.Sc. from TU Darmstadt, Germany.

The widely debated security problems of ADS-B remain, as they are caused by the inherent lack of encryption in the technology, a problem not solved by moving receivers into space. Indeed, the attack surface of satellites is as global as their increased coverage abilities. On the other hand, the added layer of receivers offers new opportunities for physical-layer verification.