16.72 Security and vulnerabilities in the ADS-B architecture

Karthik Kavassery Gopalakrishnan

March 18, 2018

1 Motivation

Automatic Dependent Surveillance-Broadcast (ADS-B) is a GPS-based, next generation surveillance technology that can help track aircraft positions with high accuracy. The device on board an aircraft obtains signals from satellites and broadcast the GPS position of the aircraft through a transmitter. First, we expand the acronym to understand the basic features:

1. The transmission is 'Automatic', meaning that the position of the aircraft will be transmitted periodically (around once every 0.5 seconds), and not necessarily in response to an interrogation.

2. It is a 'Dependent Surveillance', meaning that the position transmitted by an aircraft is not independently computed by the aircraft, but is rather dependent on the external GPS system.

3. The signals are 'Broadcasted', i.e transmitted omni-directionally and is not receiver specific.

There are two important features of this ADS-B architecture that fundamentally lead to security vulnerabilities:

1. Non-encrypted messages: The messages can be understood by any listener.

2. Non-authenticated messages: There is no way to verify the identity of the sender of the message

Finally, we would like to compare ADS-B with other surveillance methods.

- The earliest methods developed, and still in use are primary radars, where EM waves were transmitted from a ground station, reflected off the metal in a target airplane and captured by the ground station. The angle of transmission and the time lag is used to determine the range and bearing to the target. Although primary radars do not need any cooperation from the target, they have limited accuracy and do not provide reliable altitude information.

- Secondary Surveillance Systems (SSR) were the next development that led to improved precision and range for identifying cooperative targets. A transponder located on the aircraft responds to an interrogation by a ground station. The signal emitted by the transponder gives the azimuth and range. Mode C transponders also transmit pressure altitude. Mode S transponders further enable selective replies to prevent the problem of synchronous garble and correlated replies.

- Multilateration involves multiple (atleast three) ground based receivers that triangulate the location of a single signal based on arrival time-difference at these ground stations. They are currently limited to ground surveillance and certain mountainous terrain.

In this report, we wish to highlight that ADS-B alone cannot be used as a reliable and robust form of surveillance even though it is more accurate when functioning correctly. Several proof-of-concept attacks have been demonstrated by hackers and security experts and it can be expected that they may become realistic threats in the future. Currently, multiple redundant systems are used for surveillance, thus mitigating the risks associated with an ADS-B failure. However, truly realizing the potential of ADS-B and using this improved accuracy for reducing separation requirements, introducing new procedures and flying more optimal routes may require us to make changes to the open architecture.

Section 2 will summarize the attacks that have be demonstrated in the ADS-B system and Section 3 present some of the solution approaches. In Section 4, we will discuss the perspective of the stakeholders- the FAA, ATC and Pilots regarding the problem. Finally, we propose some practical changes that can be considered by the FAA in Section 5.

2 Attack strategies

In this section, we will discuss some of the ways in which ADS-B system integrity can be compromised. The strategies that we will discuss are arranged in the decreasing order of its generality. For example, all forms of wireless communications are subject to jamming by a stronger EM wave from the vicinity. On the other hand, message modification is an attack strategy that is more specific to the ADS-B network architecture. It is important to note that all these attacks have been successfully demonstrated in laboratory settings.

2.1 EM signal jamming

Jamming means that an attacker is transmitting some signal at a higher power in the same frequency as the ADS-B signals. Denote P_{PG} as the power of the ADS-B signal sent by the plane P at the ground receiver G, N_G is the nominal background noise at the ground receiver and P_{AG} as the power of the EM waves transmitted by the attacker at the ground station. Jamming can be accomplished if the transmitted signal by the attacker is white noise and $\frac{P_{PG}}{P_{AG}+N_G} < \delta$, where δ is the minimum Signal-Noise Ratio (SNR) that is required by the receiving station to decode the ADS-B message [7]. The authors of [3] demonstrated this kind of an attack using low-cost jammers.

2.2 GPS interference and spoofing

ADS-B is dependant on accurate GPS measurements taken in the aircraft. However, GPS signals can and have been compromised in the past by either interference or spoofing [5].

For instance, the FAA issued NOTAMS regularly in the 2014-16 period due to intentional jamming of GPS by North Korea. In 2013, a truck driver in Newark used a personal GPS jamming device to hide his location from his employer. This interfered with the ground based GPS augnemtation signals and lots of aircraft in the vicinity reported erronous readings. Spoofing has not been demonstrated in aviation certified GPS yet, but remains a potential concern as current avionics are not certified to withstand spoofing attacks [4]. The FAA in a 2015 report concurs that "there is potential for un-flagged, erroneous position to be output to primary flight displays."

It is important to note that the EM signal jamming attack and GPS interference/spoofing are not problems that are only affecting the ADS-B systems. They could also compromise radio aids to navigation (ILS, VOR etc) and affect flight paths in case of GPS/RNAV approaches.

2.3 Eavesdropping

Because of the non-encrypted nature of the transmissions, ADS-B messages are not private. An experiment conducted in [7] by placing a receiver on the rooftop of a 4 story building collected information about 18,554 flights in one week, which were as far as 450 km away. Using the received information and combining with publicly available data sources, one can obtain the aircraft type, its N-number, ICAO identifier, owner, origin, destination, seats, engines etc. There is consequently a loss of privacy for private aircraft operators and GA airplanes who can currently maintain anonymity by submitting a Blocked Aircraft Registration Request (BARR) to the FAA. While passive eavesdropping may not be a direct security threat, they can for the basis for more sophisticated attacks.

2.4 Message injection

In this type of attacks, the attacker injects false messages in the system. This means that the attacker transmits messages that mimic a legitimate ADS-B messages from an aircraft, and encode an aircraft identifier, speed and location information. It is possible because of lack of both encryption and sender authentication in the protocols. This attack has been successfully demonstrated in several papers [7, 1] using inexpensive, commercial, off the shelf hardware, and widely used open source software. The target of this attack is any ADS-B receiver- ground stations as well as aircraft equipped with an ADS-B In (which is used for traffic information display). The attacker may be present on the ground, or in another aircraft. When such attacks happen, ATC and other aircraft in the vicinity with a ADS-B receiver will see a new 'ghost' aircraft (which does not exist in reality) on their screens. This can cause confusions and force other aircraft to take evasive maneuvers in the face of this collision threat. In May 2017, ground testing of ADS-B equipment triggered a fake TCAS alert for an Boeing 737 on approach to landing. Although the pilot responded to the message and took appropriate evasive maneuvers, it impacted the airport operations for upto 30 minutes, leding to re-sequencing of landing traffic and causing delays (FAA service bulletin 1702). Another possibility is that the attacker can flood the radar display of the traffic controller with ghost aircraft and render the screen useless [7].

2.5 Message deletion

Messages can be deleted by either constructive or destructive interference. It is harder to achieve destructive interference because the exact inverse of the input must be transmitted. This requires precise synchronization and timing. The result of a successful destructive interference will be a signal that is highly attenuated. To delete the message via constructive interference, the synchronization requirements are less stringent and it is sufficient if a signal causes enough bits in the message to flip. The check-sum parity field in an ADS-B message contains enough information for upto 5 bits of error to be corrected. If more than 5 bits have an error, then the receiver will discard the message. If more than 5 bit errors can be consistently maintained, it can lead to aircraft disappearing from the ADS-B feed completely. Because an interference signal needs to reach the receiver to flip more than 5 bits, there are location and reaction time constraints on the attacking transmitter. Theoretical analysis shows that with reaction times seen in commercially available software defined radios, a 10 km radius around a ground station is ideal for jamming aircraft messages from all directions [7, 13].

2.6 Message modification

There are two possible methods to modify messages in wireles transmissions- bit-flop and overshadowing. Bit-flop involves selectively flipping certain bits in a message in order to modify it by transmitting appropriate interference signals. It is difficult to achieve this synchronization when considering a moving source like an airplane. Overshadowing requires the transmission of a high power alternate message such that the originl message part apperas to be noise. Overshadowing has less stringent requirements on synchronization, timing and location of attacker's transmitter. A modified message attack can create a virtual hijacking situation and cause significant increase in controller workload. A message modification attack through deletion and subsequent injection was succesfully conducted by the authors in [7].

An important point to note is that the message deletion and modification attacks that have been demonstrated in literature are not done on a full scale test-bed involving fast moving, high-altitude airplanes and actual receivers. In these scenarios, the ability to send appropriate waveform with precise synchronization and timing has not been demonstrated. The same is true for EM jamming or GPS spoofing. While they are easy to do it at ground based receivers, it is not easy to carry a device that will pass through security screening on-board an airplane. However, ground based GPA augmentation systems remain susceptible, as demonstrated by the incident involving the truck driver in Newark. On the other hand, the message injection experiments are extendable to the real world, since there are not such constraints for sending new ADS-B messages. Additionally, while I usually refer to the receiver of an ADS-B message as a ground station, it can also be another aircraft in the vicinity. While message injection is possible even for on-board ADS-B receivers, current literature does not suggest that it is possible to modify or delete message for mobile ADS-B receivers. Table 1 summarizes the ease of implementing these attack strategies.

Attack strategy	Ease of implementation
EM signal jamming	Easy
GPS interference/spoofing	Difficult
Eavesdropping	Easy (lots of info.)
Message injection	Easy
Message deletion	Difficult
Message modification	Difficult

Table 1: Practical ease of implementing the attack strategy

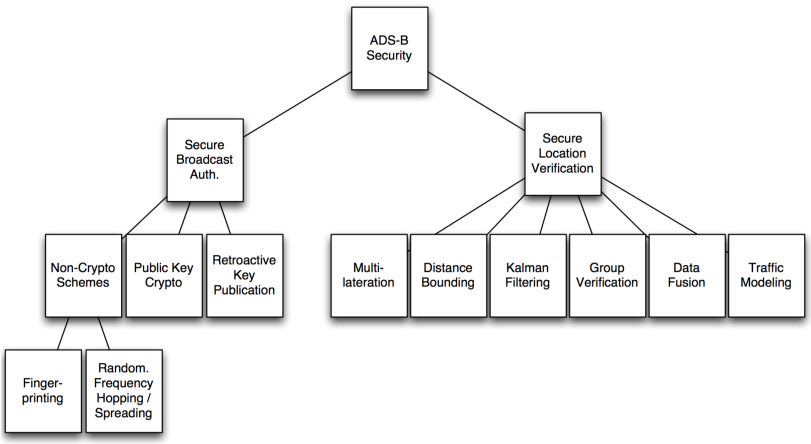

Figure 1: Taxonomy of ADS-B security [10]

3 Improving security

The previous section demonstrated the practicality and feasibility of attacks that can target the ADS-B surveillance system. We will describe some of the techniques that have been proposed in literature to mitigate the threat faced by these attacks. Figure 1 presents an overview of the security approach. In addition to the two main strategies presented by the authors (i.e secure broadcast authentication and secure position verification), it would be appropriate to add 'secure EM transmission' and 'GPS integrity' to the list. A great fraction of the research work has focused on developing light-weight cryptographic schemes that can be employed for ADS-B. However, as we shall discuss soon, it is not a realistic option given the lack of any current digital security infrastructure in the aviation industry.

3.1 Security against EM jamming attacks

There is limited work that demonstrates the use of jamming detection algorithms for ADS-B. The solution strategies depend on the type of recievers used- a single channel reciever or an array of recievers. When single recievers are used, digital signal processign techniques are employed to separate overlapping signals and obtain the original ADS-B signals. Methods that use an array of recievers have been more effective in detecting jamming, since they can use the time-diffence of arrival to know the direction of the jamming signal and filter it out with greater ease (almost 90% detection probability)[14, 3, 11].

3.2 Securing GPS integrity

Detection and compensating techniques for jamming or spoofing signals for GPS is similar to those used for EM signals. Attacks are usually carried out by a single source of EM waves. If the reciever unit can identify that there is a strong signal coming from a direction where it is not expect to see a satellite, the interfering signals can be detected. This can be done by using two omni-directional reciever units or by using a directional receiver [5].

3.3 Cryptography techniques

- *Symmetric key cryptography*: Symmetric key cryptography means that the sender and recipient share a secret key. This key is used by the sender to encode messages before transmitting it. The message that is now broadcasted is un-intelligible for anyone who does not have access to the secret key. The receiving ground station can use the key to decode and identify the aircraft position. It is important to choose a Format Preserving scheme (meaning that the length of the encrypted message is the same as the original message) such as AES (which is used by the US government for classified documents) so that we do not place any additional strain on the limited bandwidth [2, 12]. Encryption provides data confidentiality. However encryption does not guarantee integrity, meaning that there is no way to know that only the authorized sender sent the message and that it is not modified. For that, we can use a standard technique for authenticating symmetric-key messages, known as Message Authentication Code (MAC). MAC adds a short string of bits beyond the current ADS-B message length. Consequently, we can ensure the integrity and authenticity of the ADS-B messages. However, message deletion is still possible because the attacker just needs to send an interference signal for any stream of bits that is received. The biggest drawback of a symmetric encryption scheme is the aspect of key sharing and management. If the key is compromised, a new key must be shared by the involved aircraft and ground stations. There are a few options regarding how the key is distributed. They can be distributed to all or some aircraft as a part of their transponder hardware. Or it can be assigned on a per flight basis when obtaining their clearances and the assigned key can be then entered in a database that the ground stations can use.

- *Asymmetric key cryptography*: An asymmetric-key based system involves a public and private key. Consider a ground station that receives ADS-B messages. It publishes a public key, which can be used by any ADS-B broadcasting device to encrypt its message and transmit. The encrypted message is such that it cant be decoded solely by knowing the public key, ensuring the privacy of the message. The receiver uses its private key to recover the ADS-B message. Encryption alone does not prevent modification, injection and deletion of message. Digital signatures are the analogue of MAC in the asymmetric-key architecture. Together with public key encryption, it guarantees authentication and integrity of the message.

Comments on the use of encryption solution: While encryption schemes form a bulk of the literature on ADS-B security, there are few points that I would like to highlight

- Key exchange is an extremely challenging activity given the current aviation infrastructure. Questions like who will be the system administrator, will keys be hard coded or software defined, how will ground stations and other aircraft communicate the dynamically changing key list, are hard to answer

- The current protocols for transmitting ADS-B messages has been finalized and many aircraft are already equipped with the ADS-B units. Changing any protocol from the users end is impractical for atleast a few decades, given the high investment cost.

- The open nature of ADS-B in viewed by many, including the FAA as a positive feature. This was one of the requirements in the system design in order to enable aircraft-aircraft communication.

- Some security researchers have already come to the conclusion that encryption schemes are not practical and feel that it not a worthwhile direction for further research [8].

The *Non-cryptographic techniques* mentioned in Figure 1 are fingerprinting and random frequency hopping. The idea in fingerprinting is that when an external agent starts spoofing/deleting/modifying a message, there is some inherent signature of the new transmitter. This could be the small change in frequency of the transmitted message, which happens due to varying hardware specifications of different manufacturers. The idea would be to detect this minute change. Fingerprinting is a good strategy when there is a wide variety of transmitters in the market. This is unlikely given that there will only be a handful of manufacturers of aviation certified ADS-B transmitters. The other idea would be for the transmitter to hop between several frequencies in a non-predictable manner. Again, this is not an option for ADS-B given the limited bandwidth that is allocated for this purpose.

3.4 Location integrity

Methods that can verify the accuracy of the position being reported through ADS-B are described in this subsection.

- *Kalman filtering*: Since aircraft usually do not do abrupt maneuvers, Kalman filtering can be used to improve the accuracy of the ADS-B location. In addition, a multi-modal Kalman filter can also alert the user if the track does not confirm to any existing model for aircraft trajectory.

- *Data fusion*: This is the basic defense technique that the FAA is planning to rely on when ADS-B becomes fully operational. There are several redundant sources of surveillance data in the national airspace. They range from primary radars, secondary radars, wide-area multilaterational signals, filed flight plans and ADS-B.

- *Multilateration* The difference in time of arrival of a signal to different ground stations can be used to determine the location of the signal source. It is already used in some regions of the airspace and taxiways of several airports. This is a very resilient technique used for location verification as it would be impossible to spoof a location with just one transmitter, due to physical constraints on the speed of propagation of an EM wave.

Method	Privacy	Message injection	Message deletion	Message modification	Feasibility / scalability
EM/GPS protection	x	x	✓	✓	Low
Cryptographic	✓	✓	x	✓	Low
Non-cryptograhic	x	✓	x	✓	Low
Kalman filtering	x	✓	x	✓	High
Multilateration	x	✓	✓	✓	High
Group validation	x	✓	✓	✓	Low
Distance bounding	x	✓	x	✓	Low
Traffic modeling	x	✓	x	✓	High

Table 2: Comparison of solutions proposed in literature

- *Group validation*: The concept of multilateration can also be carried out by a group of recievers in the air. These receivers can be other aircraft. The idea here is that in a group of n aircraft, the $n-1$ aircraft can validate the location claims of the transmitting aircraft via multilateration.

- *Distance bounding*: This technique is again based on the physical constraint on the speed of transmission of an EM wave. When a challenger queries a target about its location, the time to receive a response Δt, gives an upper bound on the distance of the target ($c\frac{\Delta t}{2}$, c is the speed of light). In case of multiple receivers, this information can be fused together to obtain a better bound on the location.

- *Traffic modeling*: Knowledge of historical traffic density in an airspace is usually a good indicator of what the future will be, especially on IFR routes in class A airspace. When ADS-B signals report a location that has never been seen in the past, it can be flagged for further verification.

3.5 Comparison

While we presented several approaches to securing the ADS-B system, we observe that there is no single strategy that is effective against all forms of attacks. A combination of several strategies is the way to go. Another important observation is that a lot of the proposed solutions in academic literature are not feasible given the current operating environment in the aviation industry. There remains a wide disconnect between academic research and practical relevance of the proposed solutions.

Table 2 presents an overview of the solution techniques and their feasibility. We see that only cryptography techniques ensure full privacy of the transmitted messages. Almost all the methods provide some form of message authenticity or location verification to prevent modifying the reported location of an aircraft. Deletion of messages is prevented mainly when there are multiple receivers (as done in multilateration or group validation), or, jamming detection and recovery algorithms are used.

Finally, before we end the section, we comment on the ease of implementing these solutions. To protect against EM wave jamming and GPS spoofing, it is required that the on-board devices are not only equipped with software to detect the loss of integrity, but ideally have directional/multi-channel receivers. The hardware level change (which has been demonstrated to be 90% effective in detecting spoofing) is unlikely to be a mandatory requirement. As discussed earlier, the feasibility of cryptographer techniques remains

Security concern	ADS-B	Present technology (SSR)
EM signal jamming	Easy	Moderate
GPS interference/spoofing	Hard	Hard
Eavesdropping	Easy (lots of info.)	Moderate
Message injection	Easy	Difficult
Message deletion	Difficult	Difficult
Message modification	Difficult	Difficult

Table 3: Comparison of ADS-B and existing SSR vulnerabilities

low. The use of a limited number of ADS-B models and spectrum limitations makes the two non-cryptographic methods discussed (fingerprinting and frequency-hopping) unpopular. Kalman filtering is an easy to implement approach, requiring just software updates at receivers. ADS-B receivers that are currently being installed can be used for multilateration as long as they are densely spaced in order for an aircraft transmission to reach multiple ground receivers. Group validation requires a significant amount of aircraft-aircraft communication and ADS-B In installed on all participating aircraft, which is not practical to achieve. Distance bounding algorithms require an interrogate-respond format, which is done with present secondary surveillance technology, but is not possible with ADS-B, which periodically broadcasts information. Traffic modeling, although a method with limited security features, is easy to implement. To summarize, there are several solutions proposed in literature for securing ADS-B. Some of them are easy to implement, many of them are not.

4 The stakeholders perspective

The most relevant question in the discussion on ADS-B security is the perspective of the stakeholders. This includes the administrator (FAA), the air traffic controllers and the pilots.

4.1 The FAA's perspective

Given that there have been a reasonable number of demonstrated attacks on the ADS-B system, it is interesting to know the position of the FAA on ADS-B security. The FAA, in its rule titled 'ADSB Out Performance Requirements To Support ATC Service Final Rule, Federal Register,2010' states that *"using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today"*. We wish to critically analyze this statement by explicitly making the comparison between existing technology and ADS-B with regard to the attack strategies we discussed. The summary is presented in Table 3.

- EM jamming is a common problem to all radio communication systems. It is easier to jam omni-directional receivers since they are receptive to signals from any direction. This means that an attacker can be located along any direction to continuously affect the reception at the target. Directional antennas, like those used by present secondary surveillance radar (SSR) will only have interference and jamming when pointed in the direction of the attacker. It is not possible to jam it from all directions unless there are attacking transmitters physically placed all

around the rotating receiver. Hence ADS-B is more vulnerable than SSR to EM jamming.

- GPS spoofing is a more general problem that affects other aspects of navigation like way point identification, RNP routes and flight computers. The only difference is that in case of ADS-B, it also has a potential to affect surveillance. However, it remains hard to achieve GPS spoofing in any case.

- ADS-B transmits the aircraft ICAO identifier along with GPS coordinates. The ICAO identifier of an aircraft is unique, and for all US registered aircraft, the N-number, ICAO identifier, aircraft and engine type, and owner details are publicly available information. Without ADS-B, aircraft are only mandated to have Mode C transponder in controlled airspace. Mode C just transmits the transponder code. Usually the FAA gives access to the tail number that was assigned to a transponder code, and this information is combined by websites such as flightaware and flightradar24 to publish trajectories. The FAA has a 5 minute time lag before sending out this information regarding the location and tail number-transponder code mapping. It is possible for an aircraft to submit a Blocked Aircraft Registry Request (BARR) that prevents the FAA from disclosing the N-number - transponder code relationship and flight tracks from SSR. However, privacy is never fully guaranteed in either of the systems since ATC communications, where the trail number of an aircraft is mentioned can be heard by anyone with a radio receiver (http://openbarr.net uses language processing algorithms to track BARR aircraft through live ATC feeds). So ADS-B has zero privacy, while the current system has opportunities to make it harder to access details.

- Probably the most significant difference between the existing SSR system and ADS-B would be the ease of injecting fake transmissions. ADS-B message injection requires almost no sophisticated equipment, can be done with equipment less than $1000 and from any location. The injected messages will be received by airborne flights as well as ground receivers. Injecting messages in an SSR system would be very hard. A fake transmitter would only respond when there is an interrogation pulse by the ground radar and any transmission that it makes will limits its position to that particular bearing. At the most, the fake transmitter can induce artificial delay and simulate greater range. It is thus impossible to fake a moving airborne target unless the attacking transmitter is actually placed on a drone or some other mobile aerial platform.

- To successfully modify or delete aircraft transponder messages, the attacker, along with the transmitting equipment would have to be located along the line between the aircraft and the ground receiver. This is not possible for a moving target. Hence the threat of message modification and deletion for SSR does not exist. For ADS-B messages too, it is hard to practically implement these attacks, although these have been demonstrated in simple settings.

To summarize, if ADS-B alone is going to be used as an alternative form of surveillance to present technology, the FAA's statement is incorrect and does involve significantly more threats, especially with respect to message injection. However, considering that SSR systems are not going to be decommissioned and will still be actively used, there is

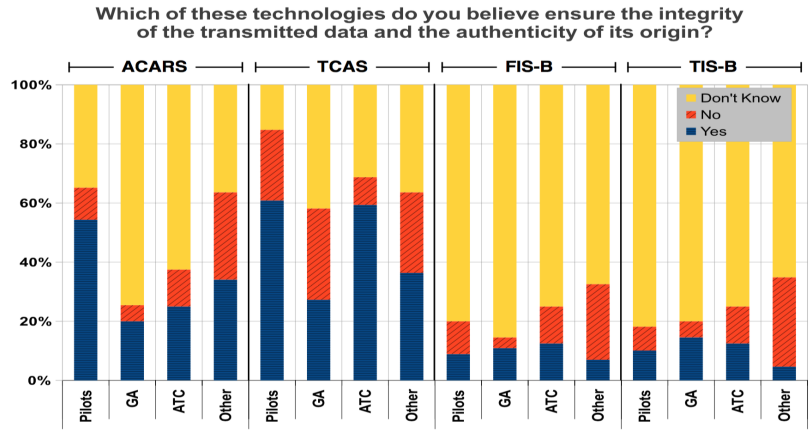

Figure 2: Authenticity of information survey results from [9]

What is the effect if...	Surveyed group	No effect	Minor loss of situational awareness	Major loss of situational awareness	Full denial of aviation service	Don't know
1) ...a non-existing target shows up on an air traffic control radar screen?	ATC	16.13%	54.84%	25.81%	0..00%	3.23%
2) ...a non-existing target shows up on a TCAS screen?	Pilots	10.75%	44.09%	31.18%	0.00%	13.98%
3) ...wrong label indications show up on an air traffic control radar screen (e.g., altitude, selected altitude, callsign)?	ATC	3.01%	28.31%	54.82%	6.02%	7.83%
4) ...wrong label indications show up on a TCAS screen (e.g. relative altitude)?	Pilots	3.23%	30.11%	51.61%	4.30%	10.75%
5) ...information or whole targets are selectively missing from an air traffic control radar screen?	ATC	6.67%	6.67%	83.33%	3.33%	0.00%
6) ...information or whole targets are selectively missing from a TCAS screen?	Pilots	6.52%	23.91%	48.91%	7.61%	13.04%
7) ...all data is missing from an air traffic control radar screen system (for example for 10 minutes)?	ATC	3.23%	6.45%	45.16%	45.16%	0.00%
8) ...all data is missing from a TCAS screen system (for example for 10 minutes)?	Pilots	6.52%	27.17%	45.65%	6.52%	14.13%
9) ...the position of an aircraft as shown to its pilot is incorrect?	Pilots	5.38%	22.58%	60.22%	7.53%	4.30%

Figure 3: Situational awareness survey results from [9]

no added risk to ATC personnel. However, the impact on pilots, who will potentially be using ADS-B In can be significant, as discussed in the next subsection.

4.2 ATC and Pilots

While the statement of the FAA on the matter of ADS-B security is clear, the opinion of air traffic controllers and pilots can be inferred from a recent study conducted in [9]. We will present and focus on two specific results that were presented in the paper.

Observation 1: Most of the pilots and controllers (almost 80%) are unaware of the possibility that TIS-B data (which is the ADS-B In data that is aggregated over the 978 and 1090 Mhz frequencies) is unverified and cannot guarantee integrity of the message (Figure 2). Among the 'aware pilots' too, less than half of them believe that the data may be non-authentic. The same is true with ATC controllers, with many of them unaware of the integrity of the TIS-B data. In fact, the survey goes one step further and highlights that it is the population of 'others', which consists of aviation and security experts who are mostly concerned about the security issues. Among the domain experts, most of the 'aware' respondents agree that TIS-B messages are potentially non-authentic and these are the individuals who are primarily vocal in highlighting this problem.

Observation 2: Although most of the pilots and controllers are unaware of the security vulnerabilities of the ADS-B system, they are unanimous in classifying the threat as significant when presented as a potential reality (Figure 3). The survey asks questions related to the exact outcome of message insertion, deletion or modification as experienced by pilots and ATC. In almost all the cases, the controllers and pilots classify these incidents as a leading to a significant loss of situation awareness. This is clearly a safety concern. A crew can easily get distracted for several minutes during critical phases of flight looking for a 'fake' aircraft which is creating a collision hazard. Similarly, controllers can end up being distracted and spending time resolving conflicts that are not even present.

We feel that most of the pilots are unaware that a problem, which they feel is serious, is moving closer to reality. As a consequence, they have not been vocal about their opinions or comments on how they wish to use ADS-B in the future.

4.3 What do we expect to see in 2020

1 Jan 2020 is the mandate in the US for ADS-B out installation to fly in most controlled airspace. With this deadline fast approaching, operators are equipping their aircraft with the required avionics. The FAA has announced no plans to decommission any existing radar facility, or to change the separation requirements or procedures after the transition. It is likely that the controllers will still be using SSR data on their radar screens, and possibly augment it with ADS-B data in congested airspace. Thus, from a controllers perspective, nothing is expected to significantly change on 1 Jan 2020. It is not clear whether the same could be said for the pilots of these aircraft. There is no mandate for ADS-B Out, but it can be expected that the number of aircraft that will equip will increase. With an increasing number of ADS-B out equipped aircraft, these ADS-B In devices will start showing reasonable traffic in the cockpit providing better situational awareness, especially to GA pilots. The human factors aspect of this technology, especially when it fails in providing an accurate description of the traffic situation is unclear.

It is worth noting that although we have discussed the security aspects of this new surveillance technology, it has been implemented succesfully, although in a small scale, as the sole mode of surveillance in he Gulf of Mexico airspace. There have been no known reports of any malicious attacks on the system.

5 Relatively easier solutions

In this section we recommend some relatively simple solutions that do not require extensive monetary investment but might still help alleviate some concerns.

1. Th primary safety concern would be if pilots start seeing incorrect information when using the ADSB-In information. Th ADS-B In information comes from two sources. One is broadcasts picked directly from other aircraft/attackers in the vicinity. The other source is TIS-B (Traffic Information Service- Boradcast), where an FAA ground station combines the data obtained from the ADS-B frequencies (978 MHz and 1090 Mhz), transponder returns and primary radar targets. The TIS-B broadcast (Figure 4) is the exact information that is available to ATC specialists. It is easier for the ground computers to process these multiple streams of information,

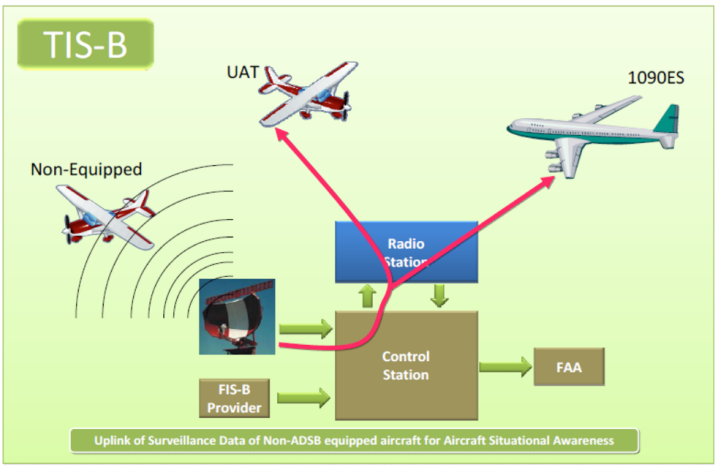

Figure 4: Traffic Information System- Broadcast architecture. Source: faa.gov

easily identify the spurious ADS-B broadcasts and only re-transmit the validated locations. If pilots use only the ADS-B information that comes from a verified ground station, it is possible to add one more layer of security. Implementing this may require some sort of preamble changes in the format of the ADS-B messages sent by the ground transmitter and a corresponding change in the software of the ADS-B In receivers. The benefit would be more reliable situation awareness for pilots.

2. Wide Area Multilateration (WAM) provides a great opportunity to confirm the position of an ADS-B message. WAM receivers are easy to install and inexpensive. They can be co-located on the ADS-B ground receivers itself. The advantage of multilateration is that these stations can be used to track non-ADS-B aircraft before equipage is attained as well as used to confirm ADS-B targets once everyone equips. In fact, it is possible that no additional receives other than the current ADS-B ones are required because all we need to do is compare the time of arrival of an ADS-B message at different ground stations to find location of the source using multilateration.

3. Specific training for pilots and controllers is needed to increase awareness of the possibility of this mode of ADS-B failure. While separation requirements have not been changed, it is important for controllers to plan for a loss of ADS-B integrity and how to revert back to Multilateration, SSR or procedural separation techniques. Pilots also need to recieve more awareness training as incidents like the fake TCAS alert for an aircraft on approach or jammed GPS signals can become more prevalent. The FAA already has taken steps in that direction by clarifying that ADSB-In data is only 'advisory in nature' and the primary mode of collision avoidance is visual scanning and separation.

4. Presently an anonymous mode of operation exists for ADS-B transmitters broadcasting on the 978 Mhz frequency. In this anonymous mode, the aircraft will receive a randomly generated ICAO address which will prevent from eavesdroppers to get the tail number and look up details. The anonymous mode does not exist for the 1090 Mhz ADS-B transmitters. Implementing this will alleviate the concerns of business aircraft operators.

6 Concluding remarks

The security threats and vulnerabilities of ADS-B has been demonstrated in several laboratory settings, and many of them are likely to become more common with time. It is clear that there is no one solution to this problem and completely fixing many of the vulnerabilities requires significant efforts in redesigning the architecture of ADS-B. This is not a practical alternative and we propose a few relatively easier options that can be considered. More importantly, the way in which the FAA plans to use ADS-B in the future- as a source of precise data to augment ground radars or as a sole form of surveillance will determine the effort put to secure the system.

An important aspect of this problem, that we did not discuss in this report is the motivation of the attackers who exploit ADS-B vulnerabilities. It is not clear what the likelihood of intentional attacks in the future is. The increasing capabilities of UAS can change these threat models pretty quickly. If ADS-B becomes the primary mode of surveillance for UAS, then there might be business and competitive advantages in trying to exploit these vulnerabilities. Further, UAS can also be used to perform attacks, like those involved for message modification and deletion more easily because of their ability to transport these transmitters to precise locations in space.

There are a few long term solutions that can be considered if the scope of ADS-B based surveillance is proposed to be expanded. They could include investing in developing a key management infrastructure, allocating greater bandwidth to enable secure communication and demanding greater equipage among the users of the NAS. The system must be resilient to failures and must gracefully degrade to backup surveillance systems, both in radar and non-radar covered airspace. However, it is important to remember a lot of the challenges related to secure communication in ad-hoc wireless networks is an active area of research and there are no trivial solutions.

In general this course project report aims to highlight the ".. obvious mismatch between security research and the aviation community concerning their approaches to the problem of air traffic communications security" [9]. Our current approach to air transportation system architecture".. do not include security by design in their specifications; instead the systems rely almost exclusively on redundancy" [9]. To build a truly e-enabled aircraft communication, navigation and surveillance infrastructure of the future, it is important to consider security as an integral part of the design process [6, 9].

References

[1] Andrei Costin and Aurelien Francillon. Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. *Black Hat USA*, pages 1–12, 2012.

[2] Cindy Finke, Jonathan Butts, and Robert Mills. Ads-b encryption: confidentiality in the friendly skies. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, page 9. ACM, 2013.

[3] Mauro Leonardi, Emilio Piracci, and Gaspare Galati. Ads-b vulnerability to low cost jammers: Risk assessment and possible solutions. In *Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), 2014 Tyrrhenian International Workshop on*, pages 41–46. IEEE, 2014.

[4] Washington Y Ochieng, Knut Sauer, David Walsh, Gary Brodin, Steve Griffin, and Mark Denney. Gps integrity and potential impact on aviation safety. *The journal of navigation*, 56(1):51–65, 2003.

[5] Mark L Psiaki and Todd E Humphreys. Protecting gps from spoofers is critical to the future of navigation. *IEEE Spectrum*, 10, 2016.

[6] Krishna Sampigethaya, Radha Poovendran, Sudhakar Shetty, Terry Davis, and Chuck Royalty. Future e-enabled aircraft communications and security: The next 20 years and beyond. *Proceedings of the IEEE*, 99(11):2040–2055, 2011.

[7] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Experimental analysis of attacks on next generation air traffic communication. In *International Conference on Applied Cryptography and Network Security*, pages 253–271. Springer, 2013.

[8] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Security of ads- b: State of the art and beyond. DCS, 2013.

[9] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. On perception and reality in wireless air traffic communication security. *IEEE Transactions on Intelligent Transportation Systems*, 18(6):1338–1357, 2017.

[10] Martin Strohmeier, Matthias Schafer, Vincent Lenders, and Ivan Martinovic. Realities and challenges of nextgen air traffic management: the case of ads-b. *IEEE Communications Magazine*, 52(5):111–118, 2014.

[11] Wenyi Wang, Geng Chen, Renbiao Wu, Dan Lu, and Lu Wang. A low-complexity spoofing detection and suppression approach for ads-b. In *Integrated Communication, Navigation, and Surveillance Conference (ICNS), 2015*, pages K2–1. IEEE, 2015.

[12] Kyle D Wesson, Todd E Humphreys, and Brian L Evans. Can cryptography secure next generation air traffic surveillance? *IEEE Security and Privacy Magazine*, 2014.

[13] Matthias Wilhelm, Ivan Martinovic, Jens B Schmitt, and Vincent Lenders. Short paper: reactive jamming in wireless networks: how realistic is the threat? In *Proceedings of the fourth ACM conference on Wireless network security*, pages 47–52. ACM, 2011.

[14] Renbiao Wu, Geng Chen, Wenyi Wang, Dan Lu, and Lu Wang. Jamming suppression for ads-b based on a cross-antenna array. In *Integrated Communication, Navigation, and Surveillance Conference (ICNS), 2015*, pages K3–1. IEEE, 2015.