International Journal of Research in Advent Technology, Vol.6, No.7, July 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Review of Vulnerabilities of ADS-B

S. Sudha Rani[1], R. Hemalatha[2]
Post Graduate Student, Dept. of ECE, Osmania University, 1
Asst. Professor, Dept. of ECE, Osmania University 2
Email: ssrani.me.ou@gmail.com 1
hemalatha.rallapalli@gmail.com 2

Abstract: Automatic Dependence Surveillance - Broadcast is now mandatory for all civil and military aircrafts with a dead line of 2020. ADS-B is signaling mechanism by which is it possible to build a vehicle-to-vehicle network and provide reduced spacing for the air traffic thereby paving the way for increased air traffic density. An ADS-B signal is transmitted by an aircraft consisting of own parameters like position of the aircraft in terms of lat, long and altitude, ground speed etc. at predefined intervals whether there is a request for transmission or not. Thus this provides visibility of the aircraft to other aircrafts and to the ground station. However, this scheme, though very accurate and beneficial for increasing the aircraft density by reducing the spacing between them, is prone to a number of attacks, and raising safety concerns. This paper brings out the vulnerabilities and possible countering mechanisms to increase the safety of the air traffic.

Keywords —ADS-B; Air Traffic Control

1. INTRODUCTION:

The Communication Navigation Surveillance (CNS) forms the basis of the Air Traffic Management. The job of CNS is to ensure that the air traffic moves smoothly and that collisions between airplanes are avoided. This is done by periodic voice and data exchange between the pilot and the Air Traffic Controller who interacts with all the air traffic and ensures a collision free movement.

CNS is mostly dependent on primary surveillance radar and the secondary surveillance radar. Independent surveillance sensors include Primary Surveillance Radars (PSR) and Secondary Surveillance Radars (SSR). In the PSR the azimuth orientation of the radar antenna provides the bearing of the aircraft from the ground station, and the time taken for the pulse to reach the target and return provides a measure of the distance of the target from the ground station. This information is presented to the Air Traffic Control on a display. However, due to inherent limitations, the PSR cannot measure the altitude of the target and the aircraft depends on barometric measurement for this purpose.

Though Primary Surveillance Radar (PSR) is the major workhorse of the ATC, and can provide independent surveillance of airspace, it has the disadvantages that the range of operation is dependent on the power transmitted and requires higher power to compensate for factors like target attitude and signal attenuation in rainy weather. DME report by the aircraft is also used in conjunction with the PSR information for identification purpose.

To overcome the problems of PSR, Identification Friend or Foe (IFF) system was developed as a means of positively identifying friendly aircraft from enemy. For civil use this is known as Secondary Surveillance Radar (SSR), which relies on on-board Transponder which when interrogated by a ground controller sends a coded reply signal. Since it is an active reply mechanism, this provides a much greater range. Every aircraft is assigned a fixed 24-bit ICAO address, which is used to identify the particular aircraft.

In view of increasing air traffic, it is required to reduce the requirements of spacing between aircrafts. To improve the air traffic density and to provide coverage in air spaces not under PSR or SSR coverage, Automatic Dependent Surveillance Broadcast (ADS-B) has been introduced as a mandatory requirement for aircrafts. The aircraft periodically broadcasts its state information, which includes horizontal and vertical position, horizontal and vertical velocity, aircraft number, whether a request for the information is made by the ground control or not.

ADS-B is **automatic** in the sense no pilot or controller action is required for the information to be issued. It is a **dependent surveillance** in the sense that the information of the aircraft is derived from a suitable high accuracy sensors on-board the aircraft. It is Broadcast every one second, whether requested for or not. [1]

ADS-B is a one-way broadcast system. Aircraft data derived from on board sensors is broadcast a plain text, unencrypted, error-code protected messages over radio transmission links once per second. Thus

this provides an RF visibility to the ADS-B signals and thereby to the aircraft. ADS-B technology uses the 1090MHz frequency band for the data transmission to ensure compatibility and as an extension to the secondary surveillance radar.

The advantages of ADS-B are many.
1. Increased safety of the air-traffic management and control. Use of ADS-B dramatically improves the situational awareness of pilots. The pilots receive the same kind of real-time air-traffic information as ATC controllers.
e.g. information about aircrafts around them, information about weather and terrain etc.
2. ADS-B allows planes to know their relative positions, without relying on an ATC to support them
3. ADS-B helps to optimise the air-traffic by providing minimum distance between them.
4. With traditional radars, the accuracy of the position depends on the distance to the plane, ADS-B provided accuracy is independent of the distance.
5. Since radars usually are not able to provide altitude information, the vertical separation between the aircrafts in flight has to be compromised and greater separation has to be provided.
6. ADS-B has much better spatial self localization capability and has an effective range of 100-200 nautical miles

Thus it can be seen that ADS-B allows optimised use of airspace by allowing reduced distance between planes. This becomes a requirement for busy airports. However, ADS-B transmissions are susceptible to various attacks which pose security risks to the aircrafts and ATCs. This paper brings the various security vulnerabilities of ADS-B signal transmissions.

2. ADS-B ARCHITECTURE:

The overall ADS-B architecture comprises of ADS-B In and ADS-B Out, which are seamlessly integrated into the aircraft avionics and in turn integrated with the CNS.

ADS-B has two modes. ADS-B-Out and ADS-B-In. ADS-B-Out periodically broadcasts position messages and ground control can use these messages for ground surveillance, for monitoring airspace with high accuracy. ADS-B-In offers airborne surveillance capability for an aircraft to receive and use position messages from neighboring nodes in airspace and airports. This permits self-separation assurance and spacing between aircraft thereby improving the traffic density.

The ADS-B Out block diagram is given in Figure 1. This is a mandatory requirement for all the aircrafts.

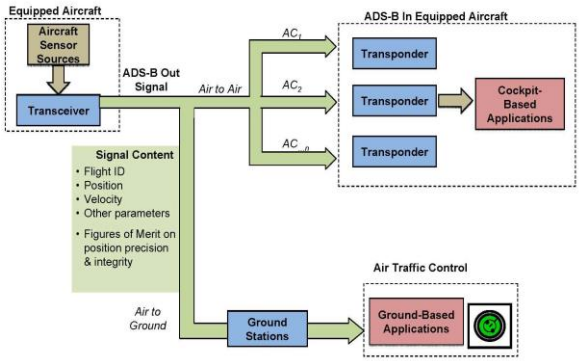

Fig. 1 ADS-B Out signal and enabled capabilities [1]

2.1 ADS-B Signal Structure :

The basic source of information for the ADS-B is the on-board sensors to derive the ADS-B information. The following figure gives the signal structure and the information carried on the ADS-B Transmissions based on the information generated by the on-board sensors. [2]

The ADS-B transmission structure consists of a preamble of two synchronization pulses. Pulse position modulation (PPM) is used as the modulation technique for transmission. Each time slot of the PPM is 1µs long, a 0.5µs pulse in the first half of the slot indicates a '1'-bit and in the second half indicates '0'-bit. Since the modulation used is PPM, it is very sensitive to reflected signals and multipath dispersion. These factors need to be considered for the vulnerabilities. Figure 2 gives the Message Format and Figures 3 and 4 give the details of the data transmitted on the message.

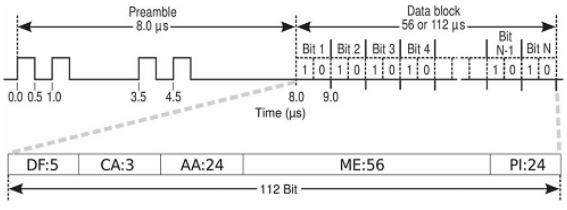

Fig. 2 ADS-B Signal structure

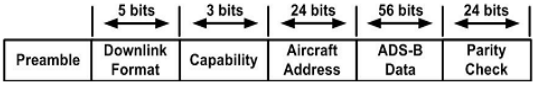

Fig. 3 ADS-B Message Format

nBits	Bits	Abbr.	Name
5	1 - 5	DF	Downlink Format (17)
3	6 - 8	CA	Capability (additional identifier)
24	9- 32	ICAO	ICAO aircraft address
56	33 - 88	DATA	Data
	[33 - 37]	[TC]	Type code
24	89 - 112	PI	Parity/Interrogator ID

Fig. 4 Signal content in the ADS-B frame

Signal content is as defined below :
1 - 4 Aircraft identification
5 - 8 Surface position
9 - 18 Airborne position (w/ Baro Altitude)
19 Airborne velocities
20 - 22 Airborne position (w/ GNSS Height)
23 - 31 Reserved for other uses

The last 24 bits are the parity bits and Cyclic Redundancy Check (CRC) is used for checking the correctness of the received message.

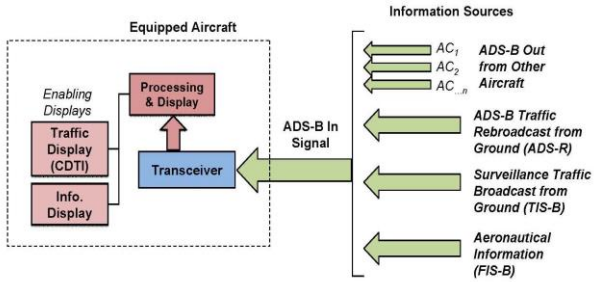

Fig. 5 ADS–B In Signal Sources and Enabled Capabilities[1]

ADS-B In refers to the mechanism, whereby the aircraft receives and processes the ADS-B signals from the ground transmitters to display the surrounding traffic and other weather information. A representation of ADS-B In is given in Figure 5. ADS–B In, thus complements ADS–B Out and provides pilots with advanced positioning information on other aircraft operating nearby, enhancing the flightcrew's situational awareness of other aircraft operating within their proximity with a high degree of precision. However, ADS-B In is not a mandatory requirement.

3. VULNERABILITIES OF ADS-B :

This section discusses the configuration of ADS-B operations, and brings out the sources of vulnerabilities in the ADS-B operations as given in Fig. 6 . These vulnerabilities lead to possible attacks on ADS-B infrastructure and compromise the aircraft safety. Various vulnerabilities and possible countering mechanisms are as follows :

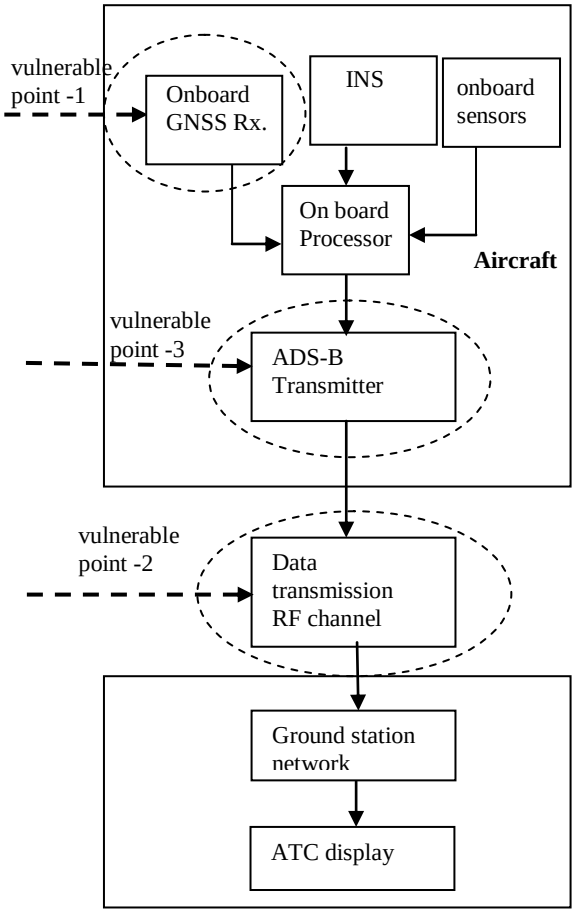

Fig. 6 ADS-B interfaces with other systems and vulnerable points

3.1 GNSS vulnerability :

The position information of ADS-B report is derived from the high accuracy Global Navigation Satellite System (GNSS) receiver on board. Therefore the safety and reliability of ADS-B technology is totally dependent on the GNSS receiver performance. This can be the major source of vulnerability of the ADS-B transmission.

GPS is based on spread spectrum and the signal level is below the noise floor. The signal to noise ratio required for processing is achieved through signal processing gain due to correlation. For the airborne GPS signal to be jammed, it requires a similar airborne platform with extremely high power or sufficient intelligence to carry out spoofing of the signal. It can be considered as a low likelihood scenario.

The unintentional vulnerabilities to the GNSS receivers may also be due to environmental conditions like solar cosmic radiation and space objects which might affect the GPS ground stations and data links.

However, the major source of vulnerability is not the spoofing of the GPS receiver, but the malfunctioning of the GPS receiver, which may be due to undiagnosed or unidentified failures either before takeoff or during flight. This is more likely event of failure and requires mechanisms to ensure that the health of the GPS receivers are monitored and ensured the correctness of GPS data before transmission.

Other onboard sensors' vulnerabilities are similar in nature and may affect wrong data being transmitted.

Countering mechanism :

Countering this vulnerability requires providing a built-in-test scheme which can provide information about the health of the receiver hardware, signal strength, data confidence level and validity of the observation information based on previous history, etc.

3.2 Data transmission RF channel vulnerability

This is the most vulnerable link in the scenario. Since the aircraft transmits the complete whereabouts of itself on the RF channel and the transmit protocol is open to all, the channel can be used to intercept and decode the signal transmission. Messages can be created or reconstructed to confuse or attack the aircraft. The following are some of the attacks possible using the RF channel as the point of vulnerability.[3]

3.2.1 Aircraft Reconnaissance:

This attack intercepts and decodes ADS-B transmissions on the RF channel. This information can be used to track the movement of assets. This is especially simple since many commercial ADS-B signal receivers like *"Flightradar"* are available at very low cost which can be used to tract the movements.

3.2.2 Ground Station Flood Denial:

This attack also aims at the RF channel and works by disrupting the 1090MHz frequency at the ground station. Since accessing the ground station from close is not difficult. a low power jamming device is sufficient for blocking legitimate ADS-B signals. The range is limited to the range of the jammer used. This is also a simple attack technique since low power jammers are easily available in open market.

3.2.3 Ground Station Target Ghost Inject

This attack is similar to the flood denial attack, but requires the generation of an encoded 112 bit message as per the ADS-B protocol and mimicking an actual aircraft movement. This results in the generation of a ghost aircraft in the ground station. This is not a simple attack and may result in adverse effects and can be a cause of safety concerns.

3.2.4 Aircraft Flood Denial:

This is similar to the Ground Station Flood Denial but carried out on an aircraft. This is a difficult attack to implement, difficulty being similar to Aircraft GPS jamming. This also requires close proximity to the aircraft and high power jammers for the attack to be effective. The other requirement is that for the attack to be continuously effective, the attack jammer should be within the range of the victim aircraft and therefore needs to continuously follow the aircraft.

3.2.5 Aircraft Target Ghost Inject

This is similar to the Ground Station Target Ghost Inject, but the target for the attack is an aircraft. In this case also, gaining access to an aircraft in flight may not be easy due to constraints listed in the above cases.

3.2.6 Ground Station Multiple Ghost Inject

This is similar to the ground station ghost attack but injects multiple aircraft signals through the RF channels. This may create a confusion state in the ground station Air traffic control. This is a very difficult attack to carry out since multiple attack messages have to generated and transmitted in such a way that they mimic a number of actual aircrafts including their speed, location and other information, requiring high processing capability.

Countering mechanism:

Countering the RF channel attacks requires a complex mechanism of authenticating the transmitted messages and secure location verification techniques as mentioned below and represented in Figure 7 :

- Multilateration, where the location of the transmission is computed based on time differences between the intercepts at distributed sensors
- Distance bounding protocol, where a limit is put on the maximum time delay between a challenge and a response based on propagation characteristics,
- Kalman Filtering, which is a predict-correct algorithm. Based on the present information, the filter predicts the arriving packet information and if the information is not as per the predicted value, appropriate measures can be taken
- Group verification done by a group of aircraft to verify location claims of non-group members in flight. Unlike multilateration, group verification operates by groups of 4 or more mutually authenticated airplanes. But this increases the complexity and requires a vehicle-2-vehicle ad-hoc network for proper functioning.

- Data fusion is a very effective way of verification, where the information generated by the primary & secondary surveillance radar are augmented with passive systems like multilateration and other authentication mechanisms
- Traffic analysis and modeling uses historical data and machine learning to create a model of a map of each ground station. This information is then used to find any abnormalities in the air traffic and air traffic transmissions.

These techniques need to be implemented at both the ground station as well as the aircraft, based on their applicability.

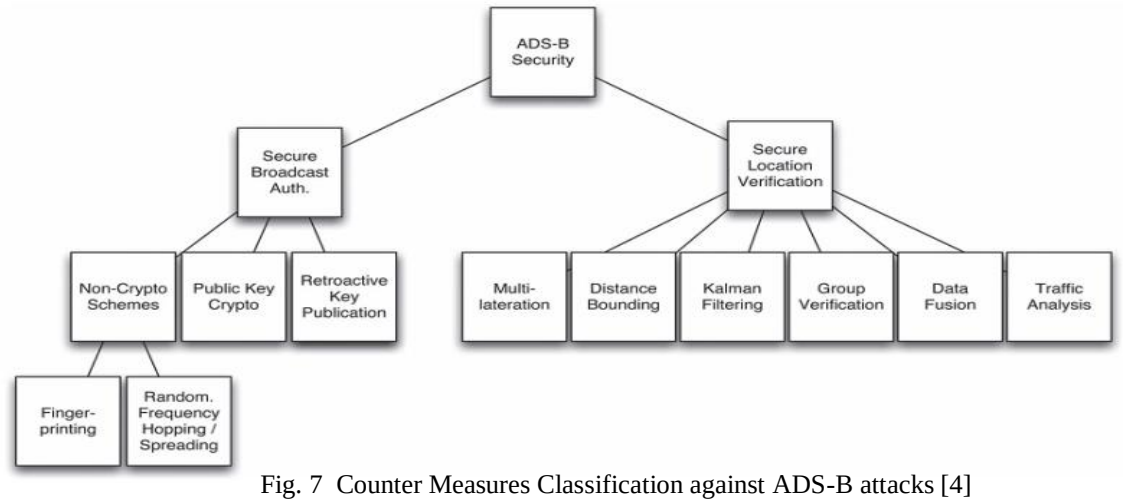

Fig. 7 Counter Measures Classification against ADS-B attacks [4]

3.3 ADS-B Transmitter as a Source of Vulnerability :

Since ADS-B itself is the source of information on which the operational infrastructure is dependent upon, the turning off of the system poses the major risk in the system, by which the aircraft is rendered invisible to the ATC which may lead to similar situations as 9-11. For this reason, overdependence on ADS-B capability of the aircraft without integrated primary infrastructure like the PSR may pose security risks and such a condition needs to be taken into account while vulnerabilities are addressed.

4. CONCLUSIONS:

This paper has brought out the general architecture of the ADS-B system and its role in the overall CNS and Air Traffic Control. Vulnerable points of the ADS-B and ground station network have been identified. Possible attacks due to these vulnerabilities have been brought out along with mitigation mechanisms to be followed.

It is also observed that, instead of using ADS-B as a standalone primary monitoring mechanism, the system should be seen integrated with the existing Air traffic surveillance mechanisms like PSR. The data generated by all the monitoring mechanisms has to be fused to provide an accurate depiction of air scenario.

5. ACKNOWLEDGMENTS :

The Authors are thankful to the Department of ECE, Osmania University for the help and support extended towards this activity.

REFERENCES:

[1] Federal Aviation Administration. (2008): Report From The ADS–B Aviation Rulemaking Committee To The Federal Aviation Administration https://www.faa.gov/nextgen/programs/adsb/media/arcReport2008.pdf

[2] Sun, J. (2017) : ADS-B Decoding Guide, Release 0.3

[3] Donald, L. (2008) : Exploring Potential ADS - B Vulnerabilites In The FAA's Nextgen Air Transportation System Graduate Research Project, USAF AFIT/ICW/ENG/11-09, Department Of The Air Force, Air University, Air Force Institute Of Technology

[4] Strohmeier, M; Lenders, V (2014) : On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials **17**(2) pp. 1066 – 1087