ADS-B: Current Flaws, Future Fixes

Timothy N. Timmons

Embry Riddle Aeronautical University
Abstract

Automatic Dependent Surveillance-Broadcast or ADS-B is one, if not the most, essential component of the FAA’s NetxGen National Airspace (NAS) transformation. NextGen is the biggest paradigm shift in the NAS since the introduction of radar following the end of World War II. The technology in ADS-B will radically change how aircraft are tracked by Air Traffic Control (ATC). Instead of interrogation by ATC radar based ground stations the ADS-B system depends on the aircraft to broadcast its position utilizing an internal GPS receiver. ATC will be able to track aircraft positions with substantially more fidelity than previously possible with radar. This fidelity promises greater airspace capacity while at the same time reducing NAS infrastructure cost by eliminating legacy radar stations. But while the benefits of ADS-B are enticing there are serious vulnerabilities that will need to be addressed. ADS-B relies on the GPS satellite constellation and the signals it produces. These GPS satellites are unprotected and vulnerable to attack by hostile and rogue nation states as well as by terrorist organizations. In addition the GPS signal is weak and susceptible to intentional and unintentional jamming. The data traffic created by ADS-B is also very vulnerable to cyber attack due to its unencrypted and open architecture. If exploited these weaknesses have the potential to wreck havoc on the NAS. Steps can still be taken to make ADS-B redundant, secure, and dependable. This paper explores the potential vulnerabilities of ADS-B and proposes several changes that can be realistically implemented to improve the system.

Keywords: ADS-B, NAS, NextGen, GPS, vulnerabilities
ADS-B: Current Flaws, Future Fixes

Automatic Dependent Surveillance-Broadcast or ADS-B is one, if not the most, essential component of the FAA’s NetxGen National Airspace (NAS) transformation. NextGen is the biggest paradigm shift in the NAS since the introduction of radar following the end of World War II. The technology in ADS-B will radically change how aircraft are tracked by Air Traffic Control (ATC). Instead of interrogation by ATC radar based ground stations the ADS-B system depends on the aircraft to broadcast its position utilizing an internal GPS receiver. ATC will be able to track aircraft positions with substantially more fidelity than previously possible with radar. This fidelity promises greater airspace capacity while at the same time reducing NAS infrastructure cost by eliminating legacy radar stations. But while the benefits of ADS-B are enticing there are serious vulnerabilities that will need to be addressed. ADS-B relies on the GPS satellite constellation and the signals it produces. These GPS satellites are unprotected and vulnerable to attack by hostile and rogue nation states as well as by terrorist organizations. In addition the GPS signal is weak and susceptible to intentional and unintentional jamming. The data traffic created by ADS-B is also very vulnerable to cyber attack due to its unencrypted and open architecture. If exploited these weaknesses have the potential to wreck havoc on the NAS. Steps can still be taken to make ADS-B redundant, secure, and dependable. This paper explores the potential vulnerabilities of ADS-B and proposes several changes that can be realistically implemented to improve the system.

System Overview

ADS-B is a key component in the NextGen implementation plan. GPS derived location information is much more accurate than current radar equipment. The FAA believes this improved accuracy will allow a decrease in the separation minimums between aircraft. This
decreased separation equates to increased capacity in the NAS and thus greater efficiency two key components in the overall NextGen plan (FAA Fact Sheet, 2010). An ADS-B ground station is also much less sophisticated and smaller than a current radar station. Both of these qualities equate to cheaper cost in installation, operation, and maintenance allowing the FAA to place greater numbers of these stations around the country. This will result in increased coverage over current radar coverage (FAA Fact Sheet, 2010).

At its essence ADS-B is an air traffic management surveillance network where the participating aircraft broadcast their horizontal and vertical position via an onboard transmitter. Radar no longer plays a role in this new paradigm. The aircraft’s ADS-B transmitter receives position data from an internal or external GPS unit. The GPS signal allows the aircraft to determine its exact location on the surface of the earth as well as its altitude. Once the system has determined its position it broadcast the information in an unencrypted digital data stream which is received not only by ground stations but also by other aircraft that are equipped with ADS-B receivers. As the systems name implies operation of ADS-B is automatic. There is no intervention required by the pilot unlike a legacy transponder which requires the pilot to turn it on, manually enter a four digit squawk code, switch to altitude reporting mode, and press the IDENT button when requested by ATC. ADS-B continually broadcasts its position once every second as soon as power is applied to the unit (Freeflight, 2011). The ground station receives the data from all broadcasting aircraft and synthesizes the data into a single overall image similar to a legacy radar display.

There are currently two types of ADS-B data link standards available: ADS-B IN and ADS-B OUT. ADS-B OUT allows for transmission of the aircraft’s position. ADS-B IN allows for the reception of additional data products such as weather and traffic data through the ADS-B
data channel. ADS-B IN is a value add capability and will not be mandatory once ADS-B-OUT becomes a requirement in 2020 ("AOPA ADS-B," 2011). There are currently two frequencies being utilized by ADS-B, 1090 MHz and 978 MHz. Because of the frequency range used by ADS-B transmitter reception is limited to line of sight (Freeflight, 2011). The 1090 MHz band is already being utilized by legacy transponders and TCAS equipment leaving little room for growth with respect to additional data products. 978 MHz on the other hand is completely dedicated to ADS-B data and has considerable growth capacity even with today’s data intensive FIS-B services (Freeflight, 2011). 1090 MHz receivers will be required above 18,000 feet while 978 MHz receivers will be limited to flights below 18,000 feet (Freeflight, 2011). The 978 MHz solution is a less expensive alternative and was chosen by the FAA for general aviation light aircraft installations (Freeflight, 2011).

As the conversion continues from radar to ADS-B the FAA has implemented a transition service labeled Traffic Information Services-Broadcast (TIS-B). TIS-B is broadcast on both 1090 MHz and 978 MHz. TIS-B imports target data from traditional radar stations into an ADS-B data stream and broadcast the information from current ADS-B ground stations. The data is received by first generation ADS-B receivers in equipped aircraft and gives the pilot the same traffic awareness that the ATC controller has. Since ADS-B is always broadcasting pilots will have increased situational awareness not only in the air but on the ground as well. Aircraft locations will be displayed on taxiways and runways ("FAA ADS-B," 2012). This capability has the potential to dramatically decrease the number of runway incursion incidents that occur each year.

In addition to traffic information the FAA has also implemented an additional service called Flight Information Services – Broadcast (FIS-B). This information contained in FIS-B
broadcast includes NOTAMS, METARs, TAFs, SIGMETS, AIRMETS, TFRs, winds aloft, PIREPS and NEXTRAD weather graphics. This additional ADS-B information is a substantial improvement over current technology. Real time weather information is currently only available with on-board weather radar. The equipment is very expensive as well as heavy thus reducing the aircraft’s useful load and performance. Pay for service Nextrad satellite weather is also available but can cost users as much as $700 a year in subscription fees. FIS-B on the other hand will be provided by the FAA for free. This information will substantially improve the situational awareness of pilots and could provide an improved level of flight safety overall as weather is a major cause of aircraft accidents ("FAA ADS-B," 2012). Only 978 MHz ADS-B IN equipment can receive FIS-B data. There is currently no available bandwidth on 1090 MHz to support the large data streams associated with the FIS-B graphical products (Freeflight, 2011). Once the FIS-B data is received it can be ported to a number of ADS-B supported display units such as Garmin glass cockpit displays and traditional rack mounted units found in many older analog aircraft.

**Implementation Timeline**

The process of implementing ADS-B started in the mid-1990s with the publication of the FAA’s Surveillance Vision Plan. The plan called for a transition from radar to satellite based surveillance. In October 2007 the FAA published a Notice of Proposed Rulemaking (NPRM) for ADS-B OUT. The FAA published a final rule for ADS-B on May 27, 2010 ("AOPA ADS-B," 2011). The rule created a ten year implementation window. As of January 1, 2020 aircraft will only be able to enter current Mode C airspace with an ADS-B OUT transmitter. Current Mode C airspace includes Class A, Class B (to include the veil), Class C (in and above), and airspace above 10,000 AGL. Interestingly the final rule did not do away with the legacy transponder and
will still require the equipment on board aircraft after the mandatory 2020 date. On the
terrestrial side of the system the FAA awarded ITT with the contract to install, operate, and
maintain the ADS-B ground infrastructure (*FAA Fact Sheet*, 2010). The FAA had implemented
80% ADS-B coverage of the United States at the end of 2011 and had established a goal of
replicating full coverage based on today’s radar footprint by the end of 2012 (*Freeflight*, 2011).
ITT will provide the ADS-B service just like a private telecom service with the FAA paying ITT
a subscription fee (*FAA Fact Sheet*, 2010). Currently there is no plan to pass this subscription
fee on to users of the NAS but with the talk of user fees in the last decade it is conceivable that
these fees could one day be passed on to aircraft operators.

When rule making was progressing on the ADS-B requirements there was considerable
push back from the general aviation community specifically recreational pilots because of the
cost of purchasing and installing a first generation ADS-B transmitter. At the time very few
manufactures were building ADS-B units because there was little demand and little reason for
aircraft owners to make the conversion. These early units were enormously expensive. The
FAA decided on a 10 year implementation plan in order to soften the time for users to transition
to the new equipment and allow the industry to ramp up production thus reducing overall cost.
With the advent of FIS-B and the free services provided the attraction of ADS-B to general
aviation pilots has increased enormously. At the same time the cost and size of ADS-B units has
decreased dramatically. The Garmin GDL 88 is a typical general aviation ADS-B unit, with an
internal GPS unit the equipment runs $5,500 (*Garmin Website,* 2012). Other less expensive
options are also available such as the Navworx ADS600-B which retails for $2,600 (*NavWorx
Website,* 2012). When additional expenses such as installation are taken into account the
typical GA pilot is still looking at a substantial investment to become ADS-B compliant.
Legacy System

ADS-B has been designed to replace the current system for tracking aircraft, radar. Radar is actually an acronym for Radio Detection and Ranging. Reflective radio waves, which radar is based on, was first discovered in 1888 (Nolan, 2011). Research in the US during the 1920s proved that radar technology had practical application with tracking ships. By the 1930s researchers were developing methods to use radar to track aircraft. Initial application was military in nature. Development greatly accelerated during WWII. The fundamental operation of radar is transmitting a radio signal into space. This signal will reflect off of any object it encounters in its line of sight. The radar station receives the reflected signal and then computes the time from transmission to reception to determine distance to the target. The ground station consists of a transmitter, antenna, receiver, and indicator. The transmitter radiates in the UHF band at power levels from 500 to 5,000 kilowatts (Nolan, 2011). Additional data processing equipment is used to process the radar signal and attach pertinent information to assist the controller in performing his/her duties. Additional information can include aircraft identification, altitude, ground speed, and directional vector arrows.

The implementation of radar across the US was starkly different than the current ADS-B transition. Radar implementation was less a strategic plan and more a hap hazard reactive response to tragic events. The CAA, predecessor to the FAA, began implementing air route surveillance radar in 1956 (Nolan, 2011). Radar technology was a result of intense military research and development that began during World War II. The original equipment was very expensive, bulky, and primitive in the picture it provided controllers. Initial implementation was slow primarily due to budgetary constraints of the CAA. It would take several high profile
accidents before adequate funding would be appropriated for the acquisition of sufficient radar stations to cover the US.

By 1961 President Kennedy ordered the now FAA to create a long-range plan for safer air traffic control (Nolan, 2011). The order resulted in Project Beacon which made several recommendations towards improving the air traffic management system and creating a more systematic implementation. Radar would evolve into two separate systems. Systems used by the air route traffic control centers (ARTCCS) would be radar data processing (RDP) while towers and approach controllers would utilize automated radar terminal systems (ARTS). In the terminal area Airport Surveillance Radar (ASR) is used. ASR has a range of 100 miles with the latest variant known as ASR-9 (Nolan, 2011). For enroute radar coverage the FAA utilizes Air Route Surveillance Radar (ARSR) which has a range of 250+ miles due to higher transmission power. The latest model in use is ARSR-4 which began to be fielded in the late 1980’s (Nolan, 2011). Radar’s inability to accurately determine an aircraft’s altitude led to the development of the air traffic control radar beacon system. This additional system is used to augment radar and relies on the aircraft’s transponder to determine the altitude of the target. ATCRBS interrogates the beacon and receives a coded signal in reply. The system operates on 1090 MHz, the same frequency that is utilized by ADS-B for aircraft that fly above 18,000 ft.

There are multiple disadvantages to the current radar systems. Radar reflects off everything it encounters. This includes terrain and buildings. This is known as ground clutter and limits how low on the horizon radar can be useful for identifying targets. Mountains also mask large portions of the Western US from radar coverage. The radar infrastructure in the United States is old and antiquated. System dependability is decreasing while the cost of maintaining this infrastructure grows with each passing year. ADS-B promises to be far superior
to radar in its ability to provide a very accurate depiction of aircraft in the sky. Despite all of the advantages there are several serious concerns with the end state once fully implemented.

**GPS Vulnerabilities**

ADS-B will rely exclusively on the satellite based GPS constellation to derive aircraft position data. GPS satellites and the signal they produce are susceptible to a host of vulnerabilities. On the extreme end of the spectrum unprotected GPS satellites are open to anti-satellite attacks by hostile and rogue nations. China demonstrated an anti-satellite attack capability in 2007 when it shot down a weather satellite orbiting at an altitude of 537 miles (David, 2007). Rogue nations like North Korea and Iran have also been actively pursuing an anti-satellite capability. While these are extreme examples GPS is susceptible to much more likely threats including environmental anomalies and terrestrial based signal jamming.

On the environmental side solar storms are one of the biggest concerns. When a solar storm occurs on the surface of the sun a large electromagnetic disturbance is created from a coronal mass ejection (CME aka solar flare) that eventually impacts the earth. These events are termed geomagnetic disturbances or GMDs. Solar storms occur roughly on an 11 year cycle (Cacas, 2012). The next storm is expected in 2013. Past CMEs have caused widespread power outages, GPS disruptions and other electromagnetic anomalies. The GPS orbital array of satellites are vulnerable to spikes of ground current that can result from GMDs interacting with the Earth’s magnetosphere (Cacas, 2012). The GMD can distort the GPS signals while they move through the ionosphere. This can lead to position accuracy errors. The US Air Force, responsible for the GPS constellation, is so concerned about solar storm activity that its Space Command focuses on the topic as part of its mission of space situational awareness (Cacas,
The FAA is also a member of the Unified National Space Weather Capability (UNSWC) along with the DOD and other government agencies which focuses in on solar storm research, forecasting, and education on dealing with post solar storm service outages (Cacas, 2012).

Solar storms occur with little warning and are global events that occur instantly. Today scientist can only provide an hour notice of a possible severe solar storm. There are already multiple instances of solar activity having an adverse impact on GPS signal availability. In December 2006 a solar event caused so much radio wave noise that GPS receivers stopped tracking the signal. This event was tracked and recorded by researchers and found to be much more disruptive to GPS than previously believed. The 2006 event occurred in a “solar minimum” period with radio noise ten times higher than previously recorded leading scientist to believe that larger outages with more frequency will occur in 2013 (NOAA news release, 2007). More recently in March 2012 a solar storm impacted satellite communications leading to the rerouting of airlines ("GPS.gov," 2012).

Electromagnetic interference originating from space is not the only concern for GPS. Interference originating from the surface of the earth can also cause service outages. The threat of interference is not only from criminal elements but can also arise from unintended consequences of legitimate and sanctioned telecommunications activity. A case in point is LightSquared Subsidiary LLC, a national telecommunications provider. LightSquared had created a wireless broadband network that was augmented by satellite coverage to provide uninterrupted service across the entire United States ("GPS.gov Lightsquared," 2012). To make the network seamless the ground based stations used the same radio band as the satellites. This band sat right next to the primary GPS band on the frequency spectrum. The implementation of the network had received FCC approval in January 2011 and was moving forward until test
reports began to show that serious disruption to the GPS signal was occurring ("GPS.gov Lightsquared," 2012). Attempts to mitigate the interference were not to FCC satisfaction and by February 2012 the agency had pulled LightSquared’s authorization for the new terrestrial network.

In this case the potential system conflict was identified before it could have an impact on NAS users, next time we may not be so lucky. LightSquared’s network would have wrecked havoc on ADS-Bs ability to accurately report the position of an aircraft. Since LightSquared’s network was national the effects would have been felt across the entire NAS, from New York to Los Angeles. Without a means of backup ATC and pilots would have had to revert to a process of reporting their positions and manually tracking those positions. In an instant the ATC system would have been set back 60 years.

The more troubling concern is the malicious jammer. Fortunately jamming, due to signal propagation and power needed, would only affect a small geographic area. But should this jamming occur in the area of a heavily trafficked Class B airspace the results could be catastrophic. It is illegal in the US to jam the GPS signal ("GPS.gov Jamming," 2011). The FCC is clamping down on the marketing, selling, and use of GPS jamming devices within the US ("GPS.gov Jamming," 2011). But despite efforts the technology exists and is available to criminals and terrorist organizations. Rogue states like North Korea have been very active in procuring and utilizing GPS jammers. A Russian manufactured truck based jammer has been shown to disrupt GPS navigation signals within a 100 kilometer radius (Gallagher, 2012). During a recent North Korean jamming attack against South Korea, 553 aircraft flying into airports at Inchon and Gimpo reported failure of GPS systems (Gallagher, 2012). These aircraft were utilizing GPS for navigation and were able to fall back on legacy systems to navigate to the
airport. Imagine if the controllers were relying on ADS-B to determine the location of the aircraft for separation purposes.

**Hacking and Spoofing the ADS-B Signal**

Another concern with the current ADS-B plan is its susceptibility to being hacked and spoofed. ADS-B data streams broadcast by transmitters are unencrypted meaning anyone with a receiver can capture the data and decode it (McCallie, 2011). In addition anyone with a transmitter can create an ADS-B data stream and broadcast it. There is also no authentication procedure in the current ADS-B transmit/receive cycle. Without authentication every broadcast is assumed to be legitimate. The lack of encryption and authentication leaves ADS-B wide open to attack by those with malicious intent.

Several computer experts have already demonstrated how the current fielded system can be spoofed. Computer security expert Brad Haines and Nick Foster built a radio capable of transmitting fabricated ADS-B signals for an imaginary airplane (Henn, 2012). Andre Costin also built a radio capable of spoofing ADS-B signals for less than $2000 (Henn, 2012). Both successful spoofs have been well documented with the information on how it was done freely available on the Internet. The creation of ghost planes can be very dangerous for those real aircraft navigating the skies. Ghost planes can cause aircraft collision avoidance systems to prompt the pilot to take evasive action. ATC may be forced to provide avoidance vectors to real aircraft moving them off their optimal flight paths and causing increased fuel burn and cost. An imaginary airplane can lead to very real consequences for real airplanes.

The FAA response to this ADS-B vulnerability has been guarded. Why the FAA did not address this vulnerability from the beginning of the program is not known. Cyber security has
become a huge focus over the last decade, especially with public infrastructure. The trend has been to hardening systems and creating more security not less. It appears to have been a massive misstep on the part of the FAA not to have built security into ADS-B from the beginning. The FAA has claimed to not have experienced a spoof attempt on ADS-B to date but considering the system is still in its infancy this claim does little to ease concerns (Henn, 2012). As recently as August 2012 the FAA stated that systems were in place to detect and remove false ADS-B signals before they could influence ATC or pilots (Henn, 2012). These systems include removing spoofed signals for an aircraft not in the geographic area. An example would be a spoofed signal transmitted in Phoenix with coordinates for an aircraft in Los Angeles. This seems less like an anti-spoof system and more like a standard quality control feature for ADS-B. Legacy radar will also be used as a secondary check to confirm the existence of an aircraft per its reported ADS-B position. This is a great solution but is really only temporary considering the FAA intends to decommission radar stations after the full roll out of ADS-B. The third system is multilateration. This technique is essentially triangulating the location of the signal and checking it against the reported ADS-B position. If the locations are substantially different than the aircraft position is deleted from the system.

Recommendations

ADS-B is the right solution for moving the NAS forward but as this paper has discussed it does have its weaknesses. These shortcomings cannot be ignored but should be clearly addressed by the FAA in its future plans as it moves forward with NextGen implementation. The fact that ADS-B transmissions are not secure is a major issue and was an enormous oversight by the initial architects of the system. It would be very difficult and costly for the FAA to change hardware standards at this point. Adding encryption and authentication procedures
would most likely go beyond just a software or firmware update and require substantial hardware modification. With ADS-B implementation already well under way many avionics manufactures already have equipment in production. Thousands of aircraft owners and operators have purchased and installed ADS-B units. There would be tremendous push back from stakeholders against such a move.

One possible solution the FAA may look at is a second generation (G2) ADS-B standard that implements message authentication and encryption into the data stream. An implementation timeline of a decade or more could soften the transition for the user community and spread the cost of modifications on the ground infrastructure side over many years. This is a standard process for the FAA when rolling out any new technology and the first generation (G1) of ADS-B is no exception. In the event that the G2 standard made G1 equipment obsolete a required compliance date of 2030 or later would allow G1 equipment owners to utilize their equipment for at least 10 years allowing for some recoupment on investment. In addition to an extended G2 implementation timeline the FAA could install interoperability hardware and software to bridge both G1 and G2 systems during the transition period. This interoperability technique is very similar to how ADS-B is currently designed to link transmissions between 978 MHz and 1080 MHz transmitters today.

Another weakness in the ADS-B system is its sole reliance on GPS satellites. The unprotected constellation is vulnerable to attack both physically and electronically in addition to environmental disruptions. Dr. Anthea Coster of the MIT Haystack Observatory summed it up in her quote “society cannot become overly reliant on technology without an awareness and understanding of the effects of future space weather disruptions” (NOAA news release, 2007, p. 1). The constellation is still relatively new, but what happens when the network ages and
satellites begin to fail? Unlike VORs you can’t send a technician in a pickup truck to go out and repair the equipment. Repairs are almost out of the question and replacement of a satellite is a multi-million dollar endeavor requiring years of planning. The effects of a GPS outage will be felt over large geographic areas with ADS-B while failure of a legacy radar station affects only a very small footprint of the NAS. Radar had redundancy in numbers. Building redundancy in positioning equipment is possible. The technology already exists today. The retaining of inertial navigation system (INS) in air carrier aircraft and the design of compact and affordable INS solutions for GA aircraft could serve as an aircraft based backup to mitigate the severity of a loss of GPS signal. A terrestrial solution could be the revival of Long Range Navigation (LORAN). In 2008 eLORAN was chosen to be the backup system to GPS but funding was cut by the Obama Administration (Poole, 2012). Revival of this effort could go a long way in providing the redundancy needed for uninterrupted ADS-B service.

**Conclusion**

ADS-B is the crown jewel in the FAA’s NextGen system. ADS-B is vastly superior to today’s current technology and is clearly moving the NAS in the right direction to ensure safety while simultaneously increasing capacity. The current ADS-B system is not without flaws and weaknesses. Fortunately the long-term implementation timeline has allowed a thorough vetting process which has brought to light many of these flaws and weaknesses. The major concerns deal with reliance on satellite navigation sources, signal jamming, and the unprotected data stream and transmission. These concerns and issues are not show-stoppers for ADS-B. There is still time to address these issues and make ADS-B better. By executing a phased implementation of ADS-B G2 over a decade the FAA can move to a more secure network with encryption and authentication. Creating or maintaining a secondary source for determining aircraft position can
ensure that a base line of redundancy exist in case of a failure of the satellite based network or jamming of the GPS signal. No complex system can ever attain perfection, ADS-B is no exception, but by making the changes described ADS-B G2 will be infinitely better than ADS-B G1. A secure and redundant ADS-B will allow the FAA and NAS users to confidently move forward with NextGen implementation confidently knowing that the system will continue to perform regardless of what challenges await in the future.
References


Information about GPS jamming. (2011). Retrieved from
http://www.gps.gov/spectrum/jamming/


Poole, R. (2012). Air traffic control reform news #93. Retrieved from


Solar storm leaves GPS service intact. (2012). Retrieved from
http://www.gps.gov/news/2012/03/solarstorm/