Addressing Operator Privacy in Automatic Dependent Surveillance – Broadcast (ADS-B)

Ryan Gauthier
Embry-Riddle Aeronautical University
ryangauthier@acm.org

Remzi Seker
Embry-Riddle Aeronautical University
sekerr@erau.edu

Abstract

We investigate security of ADS-B system and propose a framework composed of two solutions that would require minimal change to the existing system. The investigation focuses on providing an encrypted ADS-B system that provides confidentiality, availability, and integrity while requiring minimal changes to the existing ADS-B specification. The proposed framework consisting of two solutions is envisioned to be implemented through software updates while providing backwards compatibility. The most challenging requirement during this study was to work within the constraints of the existing ADS-B system.

1. Introduction and Contributions

Automatic Dependent Surveillance-Broadcast (ADS-B) is planned to be one of the pillars of the Next Generation Air Transportation System (NextGen). ADS-B lacks some capabilities that are essential for addressing cybersecurity concerns. The missing properties are source and content authentication, confidentiality, as well as integrity. The reported work has usually addressed some of these shortcomings without much consideration of others. This creates room for improvement: addressing these shortcomings collectively and this is where our work becomes relevant.

The primary goal of this effort has been to investigate ADS-B security and identify ways in which the issue of anonymity could be effectively addressed in the NextGen National Airspace System (NAS). In addition, we tried to determine whether we could devise a solution for offering an encrypted ADS-B system. Such a solution would ideally provide participants additional confidentiality and privacy, as well as some degree of message freshness and integrity.

The proposed security framework is envisioned to require minimal change to the ADS-B specification. The proposed solution is such that the system will maintain full backwards-compatibility with existing aircraft transponders and would require only software updates. Backwards compatibility would enable phased introduction of any solution in case of adoption.

The goal of this paper is not to focus on active attacks (many researchers have already covered those as seen in Section 2). This work focuses on addressing passive attacks to enhance privacy and selective anonymity against real-time tracking. If the proposed approach in this paper were to see wide adoption, it could also help mitigate various active attacks such as not being able to generate valid broadcasts.

2. Background

2.1. ADS-B Overview

ADS-B is the technology that has been heralded by the Federal Aviation Administration (FAA) and other civil aviation authorities as central to modernizing the state of airspace management across the globe [9]. It was chosen in 2005 [9] under the NextGen Air Transportation System and Single European Sky programs to improve the accuracy of radar-based traffic information used by air traffic controllers [22]. Until recently, controllers have relied on secondary surveillance radar (SSR) to improve the accuracy of aircraft identification and tracking. SSR has gone through a series of evolutions over time, as indicated by the specific mode supported by a transponder [8].

Growing airspace congestion has necessitated improvements in the types of data collected, the accuracy of that data, and the determination of data measurement error [30]. ADS-B intends to improve on its SSR predecessors in distinct ways [30]:

1. It is automatic, in the sense that no controller or pilot action is required to transmit aircraft information to nearby receivers.
2. It is dependent surveillance, in that the accuracy of transmitted information is dependent on the existence of adequate navigational information onboard the aircraft (e.g. GPS).
3. It is a one-way broadcast in nature, in the sense that aircraft information is transmitted without a priori knowledge of who will actually receive it.

URI: http://hdl.handle.net/10125/50582
ISBN: 978-0-9981331-1-9

ADS-B provides information not only about aircraft position and altitude as before, but also with regard to the identity, velocity, and intent of an aircraft [30]. This data is transmitted in plaintext, and is made available to all equipped ground- and air-based participants in an effort to address airspace congestion concerns, increase airspace coverage areas, and effectively deal with flight safety by providing pilots with access to the same information as controllers [10]. While already mandated in some other countries, aircraft within the US will not be required to adopt ADS-B until 2020 for those flights operating in or around Class A, B, C, and some E airspaces [3].

ADS-B has been approved for operation on two separate data links: 978MHz and 1090MHz. The former is referred to as Universal Access Transceiver (UAT), and is intended predominantly for use by general aviation operators. The latter, on the other hand, is generally referred to as Extended Squitter Mode S (1090ES), and is intended predominantly for use by commercial aviation operators. These distinctions reflect existing regulations already in place within the U.S., as well as those that the FAA has proposed for ADS-B equipage requirements in 2020 [3].

ADS-B services can then be further categorized into ADS-B In and ADS-B Out. ADS-B Out consists of all functionality pertaining to the automatic broadcast of aircraft parameters by participants, while ADS-B In consists of all functionality pertaining to the receipt, processing, and presentation of this information to pilots and controllers [2]. Aircraft within the U.S. will only be required to equip for ADS-B Out [3]; however, the maximum benefit can be extracted from the system through the combined use of both components to gain better situational awareness for pilots.

While ADS-B data links exist on separate frequencies, probably the most significant difference between them is the length of messages available to broadcast the same types of information to nearby aircraft. For the 1090ES data link, messages are only 14 bytes long [31], while UAT messages can be anywhere from 18-34 bytes long depending on the payload type [32]. The UAT link not only provides additional capacity to that of the already-congested 1090ES frequency, but also the bandwidth to offer ground-to-air services [2].

Table 1 shows the standard message format for the 1090ES data link. Since the 1090MHz frequency is shared with all other legacy SSR systems, an ADS-B message begins with the declaration of the ADS-B downlink format number (17). It is then followed by a description of the Mode S transponder (CA), the transponder's 24-bit ICAO address (AA), message parameters (ME), and parity check bits (PI) [31]. The limited space available to the ME field requires that aircraft broadcast several types of ADS-B messages at varying frequencies to ensure that all required information is transmitted. As stated by DO-260B, the "maximum ADS-B message transmission rate [for an aircraft] shall not exceed 6.2 transmitted messages per second" [31]. These message types include [31]:

1. Airborne Position
2. Surface Position
3. Aircraft Identification and Category
4. Airborne Velocity
5. Aircraft Status (e.g. TCAS, emergency, priority)
6. Target State and Status
7. Aircraft Operational Status

Table 1. 1090ES ADS-B Message format [8]

Bit #	*1–5*	*6–8*	*9–32*	*33–88*	*89–112*
Field |**Size**|	DF=17 |5|	CA |3|	AA |24|	ME |56|	PI |24|

By allowing for variable message lengths, UAT participants can reduce the number of messages broadcast, while still transmitting the same types of information as on 1090ES. A breakdown of the standard message format and individual message fields for UAT will not be discussed here, and we direct the reader to consult [32] for additional information.

In order to bridge the communication barrier between the two ADS-B data links, the Automatic Dependent Surveillance – Rebroadcast (ADS-R) service takes the information from each frequency and retransmits it on the other [2]. This allows each aircraft participant to not only see the aircraft that share the same data link, but also those that use the other one. The FAA also operates two other services at this time [2], the details of which are outlined extensively in [11]:

1. Flight Information Service – Broadcast (FIS-B): provides UAT-equipped aircraft with weather (text and graphics), NOTAMs, and ATIS [30].
2. Traffic Information Service – Broadcast (TIS-B): provides all aircraft with information on the approximate position, velocity, and altitude of traffic that are not equipped with ADS-B compatible transponders.

2.2. Previous ADS-B Security Analyses

General Aviation Manufacturers Association (GAMA) stated the following in its report:

"General aviation operators are concerned about potential privacy and security implications resulting from equipping their aircraft with ADS-B. … The core concern of the operator community is real-time tracking of the geographic location of a specific aircraft" [24].

In response to this and other similar concerns, the FAA working group issued the following remark:
"[We have] determined that equipping aircraft with ADS-B does not materially change the ability to track aircraft, because aircraft that currently operate with a Mode S transponder already transmit their ICAO 24-bit code" [3].

The working group was correct to point out that Mode S has already been broadcasting an aircraft's ICAO code for decades [33]. However, we believe the increased availability of technology and its impact on the privacy and security of this system requires further consideration. For example, it is trivial to lookup the ICAO code for a specific aircraft [12] online and even download the entire US aircraft registry [13]. Similarly, the decreasing cost of radio electronics has allowed websites such as FlightAware [19] and FlightRadar24 [20] to amass online tracking data by relying on a community of enthusiasts to set up their own ADS-B receivers and upload the information in real-time.

The plaintext nature of ADS-B lends itself to attacks of two kinds: passive and active. Passive attacks generally "rely on the knowledge derived by eavesdropping on ADS-B messages" [37]. For instance, long-term data collection in a given area might allow someone to come up with statistical models about destinations, delays, or fleets for not only their own business activities, but also to learn about those belonging to their competitors [37, 34]. These researchers in [37] even discovered that with a single, low-cost receiver, they could receive messages from up to 450km away and track aircraft on average for 10 minutes. Similarly, research in [39] describes a range of attacks against ADS-B system. The researchers in [21] present threat scenarios against NextGen ATC including the ADS-B concerns.

On the other hand, active attacks can "result in severe threats to air traffic safety, including attacks on air traffic monitors and automated assisting systems like traffic collision avoidance system (TCAS) and pilots" [37]. Generally speaking, most research in the area seems to agree that these types of attacks can be categorized as [35]:

1. Disruption of GPS readings
2. Wireless jamming of surveillance-related communications
3. Manipulation of ADS-B transmissions [28, 40]
    a. Message Injection (target ghost injection, flooding)
    b. Message Deletion (aircraft obfuscation)
    c. Message Modification (trajectory modification, aircraft impersonation)

Air traffic controllers are oftentimes able to utilize techniques such as multilateration [35] or even fuzzy mathematics in data fusion algorithms [16] to protect against most attacks that manipulate ADS-B communications. However, the mobile nature of an ADS-B network between any set of aircraft makes these approaches irrelevant when it comes to verifying data received by a single aircraft. It is here where security efforts need to focus, developing solutions that are not only quick and resource-efficient, but that can also deal with aircraft interactions that may only ever last several seconds [35].

Simple techniques like authentication, encryption, and hashing would be able to mitigate a lot of the issues facing ADS-B at this time; however, the consensus is that the "key distribution and management involved in [such] solutions would overwhelm the aviation industry" [28], and the message size constraints of the data links make most popular solutions to these problems undesirable or even infeasible [40].

2.2.1. ADS-B Message Encryption and Integrity

It remains a difficult problem to implement solutions that would validate and protect message contents without making changes to the data link specification. Limited bandwidth and message size are often the reason the research in this area is small, particularly with respect to 1090ES [40]. Most hashing algorithms for message integrity require space that does not exist in a message, while the key distribution problem on a congested, dynamic channel and the non-standard ADS-B message length is crippling for the purposes of encryption [1]. A proposal has been put forward by United Airlines to utilize 8 Phase-Shift Keying to expand the bandwidth of the ADS-B data link to alleviate some of these issues; however, any such changes are not expected for adoption anytime in the immediate future [24].

Given the constraints of the ADS-B system, the consensus amongst researchers is that symmetric block algorithms are the best choice when it comes to encryption [1]. In order to employ an "open" ADS-B network with asymmetric encryption, aircraft would have to be able to identify their neighbors, somehow obtain the necessary public keys, and then transmit a message several times encrypted with the public key for each neighboring aircraft [17]. This process would severely reduce the rate of information flow between aircraft on the same ADS-B data link [17]. On the other hand, use of symmetric encryption would be faster if every aircraft knew the shared encryption key for a given area [17].

The majority of solutions proposed for ADS-B suggest use of encryption for ensuring message integrity. Researchers proposed provisioning secret encryption keys for each aircraft [1, 25, 36]. These research efforts offer little value to ADS-B airborne participants for message verification, and further

emphasize the need for new approaches that allow all participants to check transmissions before processing.

A solution proposed for message integrity in [25] was that for a series of six consecutive messages, a hash-based message authentication code (HMAC) of 128 bits be determined and split across these messages within the PI field. Another solution to integrity included retroactive key publication through the μTESLA authentication protocol, which sends an encrypted message authentication code (MAC) with each transmission. The key used to generate these MACs is then periodically transmitted to all neighbors, which can then be used to decrypt them and verify that the message source has been constant over the past time interval(s) [40]. In both of these cases and in [36], supporting message integrity, changes to the ADS-B specification would have been required. Even if this were not the case, the assumption that no messages would be lost during transmission is not realistic. The likelihood of message collision on ADS-B data links quickly increases with higher traffic densities [40].

2.2.2. Other Privacy Proposals

Aside from some of these more technically oriented solutions to security and privacy concerns with ADS-B, GAMA also proposed a number of alternatives that could be utilized in the short-term [24]:

1. Private FAA Aircraft Registry: Making parts or all of the aircraft registry private would make it difficult to associate an aircraft to its owner. The problem is that the existing registry can be downloaded [13]. In addition, there are legal commitments imposed by the Freedom of Information Act exemptions and the Cape Town Convention (which established the International Aircraft Registry) [24].
2. Anonymity Mode for 1090ES: UAT provides an anonymity mode that can be utilized by pilots who operate under visual flight conditions and do not wish to utilize ATC services [15]. However, the 1090ES data link does not provide such a feature. Presumably, this is due to the fact that the target users of this link (e.g. commercial operators) require the use of ATC services during normal operations [24].
3. Aircraft Registry Privacy Office: aircraft ICAO codes are publicly available online and can be mathematically computed solely from the knowledge of a tail number. Much as in the manner that military aircraft can be issued arbitrary ICAO codes by a Department of Defense office, GAMA has proposed that the FAA provide a system by which operators could request the dynamic assignment of ICAO codes at will from a designated pool of reserved addresses [24].

There are valid concerns in [34, 15] that there needs to be a way in which any arbitrary ICAO code can still be traced back to a specific aircraft. For instance, ATC services can only be administered to aircraft whose identity is known, while search and rescue efforts could be significantly hindered if nothing is known about the aircraft itself [15]. Also, if ICAO codes are self-assigned as performed in the UAT anonymity mode, there is no longer a guarantee that these codes will be unique among aircraft [34]. A solution is needed that hides the identity of an aircraft operator from everyone except those organizations that are legally entitled to that information (e.g. FAA, government agencies).

2.3. Related Concepts

In order to properly understand some aspects of the framework presented in this paper, the reader will find it helpful to be familiar with some related concepts. Due to space constraints in this paper, we will refrain from going into too much detail; however, we urge the reader to consult the following resources for information on these topics:

1. Aeronautical Mobile Airport Communications System (AeroMACS): [5, 23, 26, 27, 29]
2. Resurrecting Duckling Paradigm: [38]

3. ADS-B Privacy Framework Proposal

3.1. Goals

At his Blackhat presentation in 2012, Andrei Costin of the Institut Eurécom described the ADS-B protocol as “all R/W with ‘Guest as Admin’ enabled” [6]. In addition to highlighting many of the issues already discussed in Section 2, he identified what he termed the dominant threats to the ADS-B system [6]:

1. Entity / Message Authentication
2. Entity Authorization (e.g. medium access)
3. Entity Temporary Identifiers / Privacy
4. Message Integrity (HMAC)
5. Message Freshness (non-replay)
6. Encryption (message secrecy)

Few efforts have simultaneously addressed most or all of these issues. Usually when a solution is proposed for an issue, it conflicts with some other issue on this list. Therefore, the primary goal for this work was to investigate the solutions already proposed for ADS-B security and adapt them into a form that is more widely functional and deployable into existing ADS-B rollouts. A secondary goal was to determine whether an effective solution could be prescribed for offering an encrypted ADS-B system in the short term.

A self-imposed constraint on our research direction was to develop a security framework that would require minimal change to the ADS-B specification. In this way, the proposed solution would maintain full backwards-compatibility with existing aircraft transponders and would require only software updates. This also means that these changes, if adopted, could be gradually phased into service across the nation and be

simultaneously administered with any existing infrastructure and protocols.

3.2. Anonymity

The fragmentation of ADS-B support across two data links has introduced a fundamental discrepancy in the length of messages supported by any ADS-B participant. For UAT, message payloads can vary in length from anywhere between 18 and 34 bytes [32], while 1090ES message payloads can only be 7 bytes (ignoring the space allocated for aircraft identity) [31]. Despite this, message source identity is established as a single 24-bit address in both ADS-B links. Typically, this value is the ICAO code for an aircraft. There are two factors that need to be kept in mind:

1. While not all UAT participants broadcast their tail number in message transmissions, 1090ES participants always do [31]. The plaintext nature of ADS-B broadcasts allows an attacker to decode and positively correlate a specific tail number to an ICAO transponder ID.
2. Even if ADS-B messages didn't transmit an aircraft tail number, the FAA provides public online and offline access to the US aircraft registry that contains all ICAO codes [12, 13]. This means that attackers can directly look up, or reverse-look up an aircraft from an ICAO code.

While anonymity is not a requirement for commercial airlines, those in general and corporate aviation tend to be more sensitive to lack of privacy. Such information could be very easily exploited via corporate espionage schemes that mine historical and live data for any trend that indicates the types of activities a competitor might be undertaking [34, 37]. So while there is more pressing demand for a resolution in the 1090ES link, any solution to this problem should be directly applied to UAT as well.

The UAT specification already provides a mechanism for pilots to achieve a form of pseudo-anonymity. As per DO-282B, there are two methods of achieving this [32]:

1. For those aircraft with an available aircraft ICAO code, a temporary identifier can be generated by XOR'ing the permanent aircraft code with the concatenated least significant 12-bits of the aircraft's latitude and longitude at the time this operation is selected.
2. For those aircraft without an available aircraft ICAO code, the time of day is used in place of the aircraft ICAO code for the operation performed in Method 1.

There are a couple of issues with this proposed mechanism for UAT anonymity. The first issue is that there is no guarantee that an anonymous aircraft code is unique. A self-assigned temporary aircraft code could collide with that of another aircraft. The second problem is aircraft tend to either operate with fairly predictable travel patterns or are based at a specific airport(s). This means that both approaches to determining a temporary address in UAT can be brute-forced by an attacker.

The general consensus in the private sector seems to be that the FAA should allocate a pool of aircraft codes that can be randomly allocated when anonymity is needed [24]. However, there has been no effective provisioning policy discussed for how the FAA should address the following issues in the context of anonymous IDs:

1. Establishing the identity of the originator for an anonymous aircraft code request.
2. The duration for which the anonymous aircraft code is valid.
3. Mechanisms for ATC to resolve an anonymous flight to a real aircraft registration.

The process of identity establishment can include:

1. The pairing of the aircraft with a personal device or electronic flight bag that is capable of connecting to FAA systems via cellular, Wi-Fi, satellite, AeroMACS, or CPDLC networks. The aircraft should "imprint" on the device (using resurrecting duckling paradigm), such that it will only ever respond to interactions with this device [38]. Since it is the communications gateway for all privacy requests to the FAA, it must be onboard the aircraft whenever in use.
2. The generation of a private-public key pair for the aircraft, of which the private key is stored onboard the aircraft and the public key is stored in a private FAA database. This establishes a trusted aircraft identity that can be used when handling requests for anonymous IDs or key schedules.
3. The generation of a binary 'case mask' for the aircraft, which is stored in a private FAA database and onboard the aircraft.

The assumption is that the FAA and its designated agents can be trusted to perform the association process stated in item 1 with the strictest of standards and integrity. It is also assumed that in case imprinting or the imprinted device fails, the aircraft can switch to its actual ICAO code. Optionally, the establishment of a power-on password would ensure that no cockpit equipment can be initialized unless the credential holder or trusted individual is present.

A secure connection needs to be established between the aircraft pilot and FAA systems to enable the identity establishment process to take place. We assume that any request shall be processed after engine

startup and cockpit equipment initialization, but before the transponder is activated. We believe that this process could be handled automatically by the onboard aircraft systems, if the pilot sets some default configuration to anonymous and/or encrypted mode.

The process of requesting an anonymous aircraft code from the FAA might look something like the following from the perspective of an aircraft:

1. Upon selection of anonymous mode, the aircraft establishes a secure connection to the FAA over its IP-enabled communication link.
2. The aircraft transmits an encrypted (symmetric) payload encrypted signed with its private key. The payload consists of:
   a. Actual aircraft tail number and ICAO aircraft code.
   b. ADS-B type (UAT or 1090ES), as this is needed to determine the length of the symmetric key required to obfuscate the true aircraft identity in all messages.
   c. A "registrant string", consisting of the publicly-available owner and address from the FAA aircraft registration record XOR'ed with the aircraft's case mask.
   d. Estimated flight time to next full-stop destination.
3. If this payload is properly decrypted and validated against known aircraft records, the FAA will provision an anonymous aircraft code and symmetric key to the requesting aircraft.
4. The aircraft receives the temporary aircraft code, an expiry time, and an encryption key. It then instructs the transponder to activate with the provided aircraft code, and use the encryption key to hide the message type (1090ES) or message field (UAT) that contains aircraft identification information.

Upon full-stop arrival at the intended destination and once the aircraft is parked, the onboard systems shall disable the transponder and inform the FAA that the temporary aircraft code can be released back into the pool. If the code expires before the aircraft makes it to the destination, the FAA shall automatically release it back to the available pool and the aircraft will reconfigure the transponder to use the aircraft ICAO code for the remainder of the flight. Any onboard TCAS systems should use the temporary aircraft code when available, but the Emergency Locator Transmitter (ELT) system should always use the aircraft ICAO code since it is intended only for operation during an emergency.

To clarify what exactly constitutes the registrant string, let us assume that we are using the aircraft with tail number N106ER to request an anonymous ID. The registration information can be retrieved online at [12].

The case mask shall be 146-bits in length. This is determined by the maximum space permitted for each of the registration fields used in assembling this registrant string, as indicated in documentation available at [13]. This concept of the case mask borrows from DNS forgery resilience research [7] to establish reasonable assurances that communication is occurring between the intended parties, particularly when that interaction is predicated on easily accessible, public information.

For this example, let us assume that the case mask assigned at aircraft delivery was:

0101101011111011000100010100101100100110110010001010110101001110010110011000111111110001011111111000010110110110011001110011100111101000111111 0101

First, we must generate the string that will be used in the XOR operation with the case mask. As shown below, it consists of the comma-separated concatenation of the registrant's name, street, city, state, and zip code. The end of the record is indicated by a period, and padded with any character to achieve a string of the maximum record length to assist in preventing brute-force attacks on particularly short aircraft records. Here, we only use the letter 'a' for simplicity.

EMBRY-RIDDLE AERONAUTICAL UNIVERSITY,600 S CLYDE MORRIS BLVD,DAYTONA BEACH,FL,32114.AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Then if we XOR the string above (x) with the case mask (c) as in $x \oplus c$, we will get the final registrant string that is transmitted along with the official request to the FAA. This XOR operation permutes the case of each letter in the string (e.g. $a \oplus 0 = a$, $a \oplus 1 = A$). While the researchers in [7] didn't account for manipulation of numbers or symbols in their paper, rules could easily be defined for these characters to further validate that the correct case mask is being used (e.g. $x \oplus 0 = x$, $x \oplus 1 = (x+1) \bmod 10$ for numbers).

Note that the field delimiters imposed on the registrant string are not part of this XOR operation, and we assume that we are using nonprescribed XOR rules for numbers and punctuation for the final output:

eMbRY-RiDDLE aERonaUticAl unIvERsiTy,600 S clYde MoRrIS BlVd,dAYTonA BEacH,Fl,32114.AAAAAaaaAaAAAAAAAAAaaaaAaAAaAAaAAaaAAaaAAAaaAAAaaAAAAaAaaaAAAAAAaAaA

For this example, we assumed that the case mask is unchanged over the lifetime of the aircraft. But, it is also possible that this element could be implemented in such a manner to provide a rotating, time-based case

mask to prevent against further tampering, brute-force, or replay attacks.

3.3. Encryption

Our secondary goal was to determine if there was an effective solution for encrypting all ADS-B links to provide additional confidentiality and privacy to participants, as well as to ensure some degree of message freshness and integrity checks. This proves much more difficult to implement, especially when considering the significant difference in space available to messages in the 1090ES and UAT links. Since UAT provides much more space and flexibility in its message format specification, most research efforts have oriented themselves around that link, almost completely ignoring the 1090ES link where such functionality would be much more desirable. Hence, we take a complementary approach and place emphasis on the more-constrained 1090ES link as our discussion can easily be extended to UAT. We also assume that any encrypted data links will implement crossover support via ADS-R for encrypted 1090ES traffic to see encrypted UAT traffic, and vice versa.

Bandwidth and resource limitations do not leave much room to utilize asymmetric encryption for encrypting ADS-B traffic. Therefore, symmetric encryption method with format-preserving properties is considered the best approach right now [17]. Researchers at the Air Force Institute of Technology determined that an encryption method named FFX-A2 [4] (for which NIST standardization is still pending) would provide sufficient entropy for the ADS-B 1090ES system, despite the number of fixed bits for any individual aircraft and its short message length [18]. However, this study left the issue of key distribution largely untouched, merely assuming that a CPDLC data link would serve the needs of key distribution for all aircraft [18].

While the CPDLC data link is certainly a viable option for key distribution, not all aircraft are configured with the necessary equipment to solely rely on this type of en route communication data link. We will describe an alternative that balances link encryption with data openness. Note that our previous approach for aircraft anonymization is fully interoperable with this idea.

A request to operate under encrypted ADS-B conditions must be approved by the FAA, and should be carried out in a manner almost identical to the process for securely carrying out authenticated requests between the aircraft and FAA systems described earlier. The request type must be differentiated and additional payload parameters would be required. A two-step process is need to obtain the keys required to participate in the encrypted link.

The aircraft performs the first step before taxi clearance is given, and is meant to obtain pre-clearance approval from the FAA to participate in the encrypted link. In addition to all parameters transmitted with an FAA request from above for aircraft anonymization in Step 2, the request for access to the encrypted data link would also include information about the flight path and any alternative routes identified due to forecasted weather along the route. Even if an aircraft encryption request is approved, no keys will be issued now. The concern is that somebody might try to gain access to encrypted transmissions by stating their intent to participate and receiving their key schedule for the route, but then not take off. So, there needs to be verification that the aircraft has indeed taken-off before the keys are transmitted to the aircraft.

The second step is key distribution, and this might be handled in one of two ways depending on the airport from which an aircraft is taking off. If departing from a controlled airport, the keys can be securely transmitted over the encrypted communication link between the FAA systems and the aircraft upon delivery of takeoff clearance or roll. However if departing from an uncontrolled airport, the keys can be transmitted to the aircraft over the same link upon confirmation of radar contact or successful ADS-B signal multilateration from a nearby ATC, Air Route Traffic Control Centers (ARTCC), or ground facility (within no more than 10 minutes after takeoff). We assume that if an aircraft takes off without successfully obtaining a key schedule, it must either deviate from its flight plan to achieve connectivity with the FAA systems or simply continue its flight in an unencrypted ADS-B mode.

The NAS is divided into several zones, named ARTCC, which are meant to handle all aircraft en route through a given geographical region. A map of the US with these zones depicted can be seen at [14].

We propose a system whereby each ARTCC zone maintains its own encrypted ADS-B network of air and ground participants, as inspired by concepts presented in [17] and [25]. Each ARTCC zone will impose a universal zone symmetric encryption key $K_{Z,T}$ on its ground stations for zone Z and time period T, which will change every hour. The rotation of this universal zone key will prevent aircrafts from overstaying their presence in an encrypted link, as well as localize the extent to which key compromise can affect communications on the ADS-B link. This key, $K_{Z,T}$, is distributed to all approved encrypted link participants at the time of the original request, whose reported route will cross into the zone for the specified time period. We assume that there is some mechanism by which these keys can be pre-determined and obtained by FAA systems for distribution in advance, such that aircraft will already have them onboard when needed. We will

also assume that these keys will be stored onboard the aircraft in such a manner that it is impractical to access by an attacker before their eventual expiration.

In addition to this universal zone key, $K_{Z,T}$, each zone will have a key used to encrypt all ADS-B traffic that changes every 15 minutes. This key is defined as K_Q for that quarter Q of the hour. Ground stations in the zone shall continuously transmit this key every 5 seconds in a specially marked ADS-B message that is encrypted by the current ARTCC zone key as follows: $\{K_Q\}_{Kz,t}$. Knowledge of the universal zone key $K_{Z,T}$ allows authorized ADS-B participants to obtain the correct key K_Q.

The authors of [18] proposed that the parity field of an ADS-B message also be encrypted for message integrity purposes; however, in the interest of maintaining backwards compatibility with older ADS-B transponders, our security framework does not observe this.

Since the confidentiality of the encrypted ADS-B link depends on the secure transmission of the key K_Q, we propose that K_Q be constructed such that the integrity of the message source can be validated. In other words, we need to ensure that we are not receiving a spoofed encryption key announcement. Let us define the following operations:

1. The ':' (colon) character defines the concatenation operation.
2. LEN(s) defines the function that returns the length (in bits) of parameter 's'.
3. HMAC(x,y) defines the cryptographic hash function that calculates the MAC for 'x' in conjunction with secret key 'y'.
4. S_N defines a binary data string of 'n'-bits.

We can then define K_Q such that:

$$K_Q = S_N : HMAC(S_N, K_{Z,T}),$$
$$\text{where } LEN(K_Q) = 80 \text{ bits.}$$

By using this approach to encryption, we would maintain the openness of ADS-B broadcast data within the encrypted link. It also ensures aircraft are bounded upwards of 1 hour, during which they could potentially still overhear any encrypted communications in that area. The selection of these time frames was arbitrary, and further modification of these time parameters could be performed to balance system performance with limiting access control, based on experimental testing or simulation.

One could argue that a known plaintext attack is possible in this network configuration. While it is theoretically possible that an attacker could modify an aircraft to obtain the ADS-B message contents prior to encryption and then use a portable receiver to collect the network traffic, it will prove difficult to correlate an encrypted message to an aircraft since the aircraft identifier field is also encrypted. Even if someone managed to figure out the pairing between plaintext and ciphertext in the ADS-B traffic, it would still be infeasible to perform the attack in the amount of time needed to manipulate communications. If we assume that some machine onboard the aircraft can generate 10^{18} ciphertexts each second and that the encryption key is 80-bits, it would take nearly 7 days to get a useful result. It is far more likely that improper handling of the secure communication channel with the FAA would be the weakest link to attack before the brute-force approach becomes feasible.

A challenge with the proposed encryption approach is if an aircraft encounters unexpected weather, emergency, or delays along the flight path. For aircraft with available en route communication links, the reason for delay can be recorded and updated keys could be issued to extend access to an ARTCC zone or to allow entry into additional zones. As an alternative for those aircraft without the necessary hardware, it might be possible to declare any possible delays or deviations in addition to the intended flight plan, so that these keys are issued at takeoff as well. Obviously, this is less desirable from a security standpoint, but it would be more practical than forcing these participants to lower altitudes or to even land at an airport to establish a new communication channel.

We expect that the implementation of encryption on top of the existing ADS-B specification will require some means of differentiating messages transmitted from aircraft operating under these conditions. This would be especially true if encrypted and unencrypted ADS-B links are operated simultaneously with one another, which is a reasonable assumption given the phased introduction of aviation technologies in the past. Encryption will obfuscate the content in the aircraft address and payload fields, resulting in content that might not make sense when processed by an aircraft without encryption capabilities. Therefore, there must be an easy way for the aircraft to differentiate between these categories of messages within the same ADS-B link.

Looking at the breakdown of 1090ES message fields in Table 1, the downlink format (DF) and Mode S transponder capabilities (CA) fields are the most likely candidates for this purpose. Upon review of DO-181E, it became quickly apparent that repurposing the CA field bits would interfere with our intent to maintain backwards compatibility with TCAS [33]. However, the specification also indicated that of the 25 allocated downlink format numbers, only 12 have been officially provisioned and 13 are still available for alternative purposes [33]. 1090ES ADS-B currently utilizes two downlink formats: 17 (airborne participants) and 18 (ground participants) [31]. An additional two downlink

formats can be drawn from this pool of available numbers to distinguish encrypted messages from unencrypted ones, while still using the same underlying message format specification.

This is the most desirable solution for this problem, as it will require no software upgrade to those aircraft that do not intend to participate in encrypted data links. Their equipment will simply see the new downlink format and ignore it, because the format was not provisioned in the DO-181 specification version used at that time to write the software. However, this does mean that while all aircraft participating in an encrypted link will be able to see the unencrypted transmissions, the reverse will not necessarily be true. Future investigation will be required in this area to see if that gap could be bridged without giving the illusion that there are twice as many aircraft in the sky as compared to the actual airspace.

There is another potential problem with the encryption method discussed above when operating near ARTCC zone boundaries. Specifically, an aircraft encrypts its ADS-B transmissions using the encryption key for the zone that it is currently flying over. However, if another aircraft across the border of a zone received that message, it would not be able to know which encryption key to use to process the contents. This degrades the integrity and quality of information received over an encrypted data link in this scenario, and represents another area of future research to see if a solution might be devised. For instance, if the capability field in the 1090ES message could be repurposed, aircraft could use graph coloring of ARTCC regions in the US to encode which zone's encryption key was used to encrypt the message in conjunction with the aircraft's current location.

4. Conclusion

At the onset of this work, we sought to develop effective and practical solutions to the issues of privacy and security within the ADS-B protocol. In addition to this, we also sought to minimize the number of changes required to the specification itself in order to maximize the number of aircraft that will be capable of taking advantage of the benefits provided by these proposed improvements. It remains to be a challenge to come up with a solution that would balance between addressing the relevant issues.

We proposed an ADS-B security framework composed of two solutions. The first solution dealt with the issue of anonymity. The solution outlined a process whereby the identity of the operator requesting a temporary aircraft code could be verified, and how these codes could be provisioned and managed by civil aviation authorities to offer operators environmental and proximal privacy, while maintaining the ability of controllers and agencies to positively identify these aircraft while en route. The previous research efforts that offer anonymity in using ADS-B have focused on devising their solutions for UAT, which provides much more space and flexibility in its message format specification. Because any proposed solution needs to work for both UAT and 1090ES, we devised our solution for the more constrained 1090ES link. Our solution easily extends to UAT.

The second solution dealt with the issue of encrypting the ADS-B data link. The solution described a method of separating the NAS into individual encrypted regions that coincide with existing ARTCC areas, and managing key distribution in each of these zones to maintain the principle of ADS-B situational openness between encrypted participants.

It is yet to be determined whether the security framework outlined within this paper is the "best" approach for addressing anonymity and encryption issues in ADS-B. Further analysis and auditing of the underlying methods and processes are required.

5. Acknowledgement

The authors would like to thank the anonymous reviewers for their constructive comments and suggestions, which helped us to improve the paper.

6. References

[1] S. Amin, T. Clark, R. Offutt, and K. Serenko, "Design of a cyber security framework for ADS-B based surveillance systems," in Systems and Information Engineering Design Symposium, Charlottesville, 2014, pp. 304-309.

[2] Avidyne Corporation. (2012) ADS-B Overview. [Online]. http://www.avidyne.com/publications/guides/ADS-B-Overview.pdf

[3] W. Bellamy III. (2015, April) Equip 2020: The Latest on ADS-B Equipage, Pricing, Privacy Issues. [Online]. http://www.aviationtoday.com/the-checklist/Equip-2020-The- Latest-on-ADS-B-Equipage-Pricing-Privacy-Issues_84849.html

[4] M. Bellare, P. Rogaway, and T. Spies, "The FFX Mode of Operation for Format-Preserving Encryption," University of California, Voltage Security, 2010.

[5] J. Budinger, "Aeronautical Mobile Airport Communications System (AeroMACS) for Access to SWIM," Federal Aviation Administration ; National Aeronautics and Space Administration, Washington DC, Presentation 2010.

[6] A. Costin. (2012, July) Ghost is in the Air(Traffic): Security Aspects of ADS-B and "Flying" Technology. Video.

[7] D. Dagon, M. Antonakakis, P. Vixie, T. Jinmei, and W. Lee, "Increased DNS Forgery Resistance Through 0x20-Bit Encoding: SecURItY viA LeET QueRieS," in Proceedings of the 15th ACM conference on Computer and communications security, Alexandria, 2008, pp. 211-222.

[8] European Organization for the Safety of Air Navigation. ADS-B for Dummies: 1090ES. [Online].

http://www.ssd.dhmi.gov.tr/getBinaryFile.aspx?Type=3&dosyaID=195

[9] Federal Aviation Administration. (2014, August) NextGen Programs: ADS-B General Information. [Online]. http://www.faa.gov/nextgen/programs/adsb/general/

[10] Federal Aviation Administration. NextGen Programs: ADS-B FAQs. [Online]. http://www.faa.gov/nextgen/programs/adsb/faq/

[11] Federal Aviation Administration, "Surveillance and Broadcast Services Description Document," Surveillance and Broadcast Services (SBS) Program Office, Washington DC, SRT-047, 2011.

[12] Federal Aviation Administration. (2015) FAA Registry: N-Number Inquiry. [Online]. http://registry.faa.gov/aircraftinquiry/NNum_inquiry.aspx

[13] Federal Aviation Administration. (2015, November) Aircraft Registry: Releasable Aircraft Database Download. [Online] http://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/releasable_aircraft_download/

[14] Federal Aviation Administration. (2005, December) Tfrmap.jpeg. [Online]. https://commons.wikimedia.org/wiki/File:Tfrmap.jpeg

[15] Federal Aviation Administration, "Advisory Circular: Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems," Washington DC, AC 20-165, 2010.

[16] Z. Feng and Z. Xuejun, "An Application of Fuzzy Mathematics in ADS-B Data Validation," in International Conference on Intelligent Computing and Intelligent Systems, vol. 3, 2010, pp. 882-886.

[17] C. Finke, J. Butts, and R. Mills, "ADS-B encryption: confidentiality in the friendly skies," in Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, Oak Ridge, 2013.

[18] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the Security of Aircraft Surveillance in the Next Generation Air Traffic Control System," in International Journal of Critical Infrastructure Protection, vol. 6, 2013, pp. 3-11.

[19] FlightAware. (2015, August) FlightFeeder - Network ADS-B Receiver. [Online]. http://flightaware.com/adsb/flightfeeder/

[20] FlightRadar24. (2015) Add Coverage. [Online]. http://www.flightradar24.com/add-coverage

[21] C. Giannetto and G. Markowsky, Potential vulnerabilities of the nextgen air traffic control system. In Proc. of the International Conference on Security and Management, January 2014.

[22] Garmin International. (2015) ADS-B Academy: FAQs. [Online]. http://www.garmin.com/us/intheair/ads-b/seven-questions/

[23] D. Gray and Nima PourNejatian, "AeroMACS: Delivering Next Generation Communications to the Airport Surface," WiMAX Forum Aviation Working Group, Clackamas, 2015.

[24] J. Hennig, "Aircraft and Operator Privacy - Implications from Mode S Transponders and ADS-B for Civil Aircraft," General Aviation Manufacturers Association, Washington DC, 2015.

[25] T. Kacem et al., "Key Distribution Mechanism in Secure ADS-B Networks," in Integrated Communication, Navigation, and Surveillance Conference, Herdon, 2015, pp. P3-1 - P3-13.

[26] R. J. Kerczewski, R. D. Apaza, and R. P. Dimond, "AeroMACS System Characterization and Demonstrations," National Aeronautics and Space Administration, Cleveland, Document 2013-216497, 2013.

[27] L. Korowajczuk, "AeroMACS Applications and Lessons Learned: Network Design Considerations and Deployment Concerns for a Ground Aircraft Communication System," CelPlan Technologies, Brussels, Presentation 2014.

[28] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air traffic transportation system," in International Journal of Critical Infrastructure Protection, vol. 4, Dayton, 2011.

[29] K. Morioka et al., "Basic Characteristic Evaluation of AeroMACS Prototype System in Sendai Airport," in Integrated Communication, Navigation, and Surveillance Conference, Herdon, 2015, pp. R3-1 - R3-8.

[30] RTCA, Inc., Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B), June 25, 2002.

[31] RTCA, Inc., Minimum Operational Performance Standards for 1090 MHz Extended Squitter ADS-B and TIS-B, December 2, 2009.

[32] RTCA, Inc., Minimum Operational Performance Standards (MOPS) for Universal Access Transceiver (UAT) Automatic Dependent Surveillance - Broadcast (ADS-B), December 2, 2009.

[33] RTCA, Inc., Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System / Mode Select (ATCRBS / Mode S) Airborne Equipment, March 17, 2011.

[34] K. Sampigethaya and R. Poovendran, "Privacy of Future Air Traffic Management Broadcasts," in Digital Avionics Systems Conference, Orlando, 2009.

[35] K. Sampigethaya, R. Poovendran, and L. Bushnell, "Assessment and Mitigation of Cyber Exploits in Future Air Surveillance," in Aerospace Conference, Big Sky, 2010, pp. 1-10.

[36] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B Research," in 25th Digital Avionics Systems Conference, Portland, 2006, pp. 1-7.

[37] M. Schafer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication," in Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Michael Jacobson et al., Eds. Banff, AB, Canada: Springer Berlin Heidelberg, pp. 253-271.

[38] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," in Security Protocols: 7th International Workshop, Bruce Christianson et al., Eds. Cambridge, UK: Springer Berlin Heidelberg, 2000, pp. 172-182.

[39] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, Realities and challenges of nextgen air traffic management: the case of ADS-B. IEEE Communications Magazine, 52(5), 2014, 111-118.

[40] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," in IEEE Communications Surveys & Tutorials, vol. 17, 2014, pp. 1066-1087.