Enhancing the security of aircraft surveillance in the next generation air traffic control system

Cindy Finke, Jonathan Butts*, Robert Mills, Michael Grimaila

Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA

ARTICLE INFO

Article history:
Received 28 December 2012
Accepted 15 February 2013
Available online 20 February 2013

Keywords:
Air traffic control
ADS-B
NextGen
Format-preserving encryption
FFX algorithm

ABSTRACT

The U.S. air traffic control system is reliant on legacy systems that artificially limit air traffic capacity. With the demand for air transportation increasing each year, the U.S. Federal Aviation Administration has introduced the Next Generation (NextGen) upgrade to modernize the air traffic control system. Automatic Dependent Surveillance-Broadcast (ADS-B), a key component of the NextGen upgrade, enables an aircraft to generate and broadcast digital messages that contain the GPS coordinates of aircraft. The incorporation of ADS-B is intended to provide enhanced accuracy and efficiency of surveillance as well as aircraft safety. The open design of the system, however, introduces some security concerns. This paper evaluates the limitations of the legacy systems currently used in air traffic control and explores the feasibility of employing format-preserving encryption, specifically the FFX algorithm, in the ADS-B environment. The ability of the algorithm to confuse and diffuse predictable message input is examined using message entropy as a metric. Based on the analysis, recommendations are provided that highlight areas which should be examined for inclusion in the ADS-B upgrade plan.

1. Introduction

Despite the economic turmoil in the United States and abroad, air travel and transportation have only seen modest drops in activity. The most recent U.S. Federal Aviation Administration (FAA) report [1] notes that civil aviation contributes $1.3 trillion annually to the national economy, earning upward of $397 billion or about 5.2% of the gross domestic product. The aviation industry generated more than 10 million jobs in 2009 alone and in excess of 730 million passengers utilized air travel in 2011. Additionally, 26 cargo-only carriers operate within the nation’s airspace to transport freight and mail; UPS announced that its aircraft hauled an average of 2.2 million packages in 2012 [20]. The United States is so heavily reliant on the air transport industry that the Department of Homeland Security has identified aviation as a key component of the transportation critical infrastructure sector.

With the constant demand for faster travel and package delivery, the volume of air traffic is expected to increase considerably. In 2011, air traffic control centers handled 41.2 million aircraft, and this number is expected to increase by 50% over the next 20 years, significantly stressing the air traffic control system [7]. For reasons of efficiency and cost savings, flights are expected to bypass the established airline hubs around which the air traffic network is currently structured. The resulting concerns about air traffic safety have provided the impetus to adapt the air traffic network and upgrade legacy air traffic control systems under the Next Generation (NextGen) plan.

The proposed changes include the upgrade to the Automatic Dependent Surveillance-Broadcast (ADS-B) system. The upgrade, however, introduces potential network-wide vulnerabilities. This paper assesses the current state of the air traffic control system, identifies the security risks
inherent in the ADS-B upgrade and evaluates a security solution designed to provide confidentiality for aircraft surveillance activities.

2. Background

The current air traffic control system is antiquated and is in need of an upgrade to meet the expected growth and safety considerations. This section evaluates the current state of the air traffic control system and discusses the FAA’s NextGen plan and the associated vulnerabilities.

2.1. Air traffic control

The national airspace system is a complex system-of-systems designed to monitor and control the U.S. airspace. Aircraft typically fly predefined routes called “airways” that are designed to connect heavy traffic regions as efficiently as possible, while ensuring adequate radar coverage for monitoring traffic. Prior to takeoff, an aircraft is assigned a route comprising specific airways to follow to its destination. The route is updated as necessary during flight to avoid hazardous weather or congestion.

Presently, air traffic controllers monitor radar displays and provide positive control over the movement of aircraft to ensure safe separation. When an air traffic controller detects a potential conflict, navigational direction is provided to aircraft crews to restore safe separation. The directions and clearances are given via voice transmission over line-of-sight radio channels.

Although the air traffic control system operates in a satisfactory manner, it is by no means optimal and will be unable to accommodate the expected growth. Aircraft tracking and identification rely on outdated and unreliable surveillance radars. Indeed, primary and secondary surveillance radar have been the primary means of tracking aircraft since the late 1940s; the last significant air traffic control upgrade occurred in the 1970s [14]. Additionally, restricting flights to pre-determined airways is inefficient and imposes limitations on the density of air traffic.

Air traffic controllers depend on restricted communications to disseminate control messages. Frequent transmissions can potentially saturate the control frequencies. In busy sectors, controllers use multiple frequencies to receive concurrent communications from multiple aircraft, but such multitasking is constrained by human limitations. Human controllers are also subject to natural limitations (e.g., fatigue and information overload) and are susceptible to errors. As a result of these deficiencies, separation standards require artificial safety margins that, in turn, limit air traffic capacity.

2.2. NextGen security concerns

To overcome the aforementioned limitations, the FAA has introduced the NextGen upgrade [6], a comprehensive strategy to overhaul the air traffic control system. The strategy includes transformational programs for data communications, collaborative air traffic management technologies, and network-enabled weather information.

One of the most significant changes is the inclusion of the ADS-B system. ADS-B enhances surveillance capabilities and nearly eliminates the need for voice communications. Once it is fully implemented, the ADS-B system will enable the inclusion of more automated control systems, reducing the impact of human error and optimizing aircraft safety margins and efficiency [6].

The concept of automatic dependent surveillance (ADS) was introduced in the 1980s. The International Civil Aviation Organization has proposed the use of ADS technology in the future air navigation system (FANS) [4], which is focused on improving the communications, navigation and surveillance techniques employed in air traffic management. The vision includes improved navigation techniques using accurate satellite-based technology (i.e., GPS) and enhanced surveillance achieved by downlinking satellite-derived positions.

The term “automatic” in ADS means that pilot action is not required, “dependent” refers to the reliance on GPS technology to derive aircraft position and “surveillance” denotes the primary intended functionality [10]. ADS messages consist of data fields that specify information about aircraft position (i.e., latitude, longitude and altitude) and identification (i.e., aircraft-specific call sign). These messages are transmitted by aircraft at random intervals averaging two messages per second [15].

Message transmissions may be monitored by any receiver within range—there is no message confidentiality. The FAA has mandated that all air traffic be ADS-B compliant by 2020; this would enable any party—authorized or not—to monitor, with precision, the location of air traffic [6]. The lack of message confidentiality on the part of the ADS-B system has raised concerns among military, law enforcement and homeland security entities, all of which have secrecy and operational security requirements, but have to operate within the FAA-controlled airspace. Imagine the potential security risks of having Air Force One having to announce its exact location to any and all listeners.

The use of plain text (i.e., unencrypted) broadcasts enables ADS-B messages to be replicated. Recent research has demonstrated that it is possible to create and broadcast false messages with relative ease using inexpensive equipment [3,12,19]. Consider a scenario in which an aircraft controller’s display shows a host of ghost aircraft—at best, this would create confusion and costly delays; at worst, it could lead to aircraft accidents [14]. In response to recent ADS-B hacker demonstrations (see, e.g., [3,19]), the FAA claims to have developed a comprehensive security action plan. However, the pertinent details of the plan are security sensitive and have not been released to the public [8].

Incorporating message encryption schemes could reduce the likelihood of false message broadcasts, ameliorate the resulting controller confusion, and assist in systemwide authentication. Additionally, message confidentiality would prevent aircraft surveillance by unauthorized entities.

2.3. Related work

Little research has focused on ADS-B security and, specifically, ADS-B message encryption. Samuelson et al. [21] have proposed techniques for enhancing the overall security of
ADS-B. These include a message authentication code algorithm that provides message authentication and an encryption scheme that safeguards message content. To accomplish the latter, Samuelson et al. suggested a symmetric scheme in which the same key is used for message encryption and decryption. Due to the small length of ADS-B messages, they dismissed the use of an asymmetric cryptosystem with individual public/private key pairs, unless it is used to establish session keys. Jochum [9] offered a similar recommendation after investigating the feasibility of encrypting ADS-B messages for military applications. However, neither Samuelson et al. nor Jochum identified a specific encryption algorithm.

Unlike Samuelson et al. [21], who focused on universal access transceiver (UAT) datalink messages broadcast on the 978 MHz channel, we exclusively focus on formatted extended squitter messages that are transmitted on the 1090 MHz channel—the FAA standard [5]. These messages exist in many forms, including the military-only DF-19 messages [9]. However, we only consider DF-17 formatted messages, and, more specifically, the associated airborne position messages that are intended to be used by all air traffic. DF-17 messages are strictly formatted and are smaller than the UAT messages, providing additional algorithmic restrictions.

From here on, the term “ADS-B messages” refers to 1090 MHz DF-17 position messages. We extend previous work by specifying a suitable encryption algorithm and testing its performance in a representative ADS-B environment.

### 2.4. Feasibility of encryption

Employing encryption in the ADS-B system is by no means trivial; the system specifications impose restrictions on message length that must be observed. The unique, predefined format of ADS-B broadcast messages presents a perfect testbed for format-preserving encryption (FPE). Format-preserving encryption algorithms are designed for fixed length messages that do not conform to standard block sizes (e.g., 64-bit or 128-bit blocks); the algorithms have been used to safeguard credit card or social security numbers [1]. The ADS-B message format includes a similar non-standard count of 112 bits. Format-preserving encryption algorithms are best adapted from conventional symmetric block ciphers and have been shown to be just as secure as the underlying ciphers [2].

Key management is a difficult problem in a symmetric cryptosystem, more so because a single key leak compromises the entire system. Indeed, this is a major hurdle that must be overcome before considering the use of a symmetric cipher in a highly distributed system. Although the air traffic network is highly distributed, a symmetric encryption scheme can be implemented in a feasible manner within a controlled subset of the air traffic. For example, a symmetric system is effectively employed by the military to encrypt Identification Friend or Foe (IFF) Mode-4 transmissions. An ADS-B solution, designed to provide surveillance confidentiality, may be modeled after this case.

### 3. FFX algorithm

At this time, the National Institute of Standards and Technology (NIST) does not support any format-preserving encryption algorithms. However, the FFX algorithm was proposed to NIST in 2010, and is expected to be ratified although no published use cases currently exist. FFX stands for format-preserving (F), Feistel-based encryption (F) with multiple implementation variances (X) [1].

The FFX-A2 instantiation of FFX is specifically designed for binary strings of 8 to 128 bits. The parameters for the ADS-B implementation are derived from the FFX-A2 scheme as demonstrated in Table 1. The algorithm for encrypting ADS-B messages includes user-defined parameters: radix (i.e., character alphabet), message length, key, tweaks (i.e., logical positions of the data block), number of Feistel rounds, and the split number to delineate Feistel pairs.

Fig. 1 shows three rounds of the FFX algorithm using method = 2 alternating Feistel behavior. During each round, a part of the input, determined by split(n), is altered by the function F and then added to the remaining input. This process is repeated a total of rnds(n) times.

The function F invokes a user-determined symmetric block cipher to produce a replicable hash-like value. The developers of the FFX encryption scheme recommend that F invoke the cipher block chaining message authentication code (CBC-MAC) mode of the Advanced Encryption Standard (AES) algorithm as illustrated by the pseudocode in Fig. 2. Note that in Fig. 2 and throughout the paper, $[s]$ denotes the i-byte string that encodes the number s.

The function F requires four parameters: (i) message length n; (ii) tweak T; (iii) round number i; and (iv) message half B. The parameters are used to construct two 128-bit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>radix</td>
<td>2</td>
<td>Alphabet is 0,1</td>
</tr>
<tr>
<td>lengths</td>
<td>$n = 104$</td>
<td>Permissible message length</td>
</tr>
<tr>
<td>keys</td>
<td>$[0,1]^{128}$</td>
<td>128-bit AES keys</td>
</tr>
<tr>
<td>tweaks</td>
<td>BYTE $\leq M$ where $M = 2^{36} - 1$</td>
<td>Tweaks are arbitrary byte strings</td>
</tr>
<tr>
<td>method</td>
<td>2</td>
<td>Alternating Feistel</td>
</tr>
<tr>
<td>split(n)</td>
<td>$[n, T] = 52$</td>
<td>Maximally balanced Feistel</td>
</tr>
<tr>
<td>rnds(n)</td>
<td>12 if $32 \leq n \leq 128$</td>
<td>From entropy-based Feistel</td>
</tr>
</tbody>
</table>
strings, P and Q. The P string comprises FFX-A2 parameters and length of the tweak in bytes (t). The Q string comprises the tweak, round number and message half B. Zeros are used as necessary to pad Q to meet the 128-bit requirement.

The CBC-MAC is computed by concatenating P with Q. AESK(P XOR 0) is first calculated to determine X. Next, AESK(Q XOR X) is computed. Finally, F returns the determined number of least significant bits from the CBC-MAC computations.

4. ADS-B application

The format of the airborne position message is shown in Fig. 3. The 112 bits (14 bytes) are divided into five fields: (i) downlink format (DF); (ii) capability (CA); (iii) address announced (AA); (iv) message extended squitter (ME); and (v) parity/identity (PI) [15]. The DF field describes the message format and, as the name implies, is coded as decimal 17 (10001 in binary). These bits must remain unencrypted so that each message may be identified as a position report. The other fields may be encrypted. However, the CA field, which is used to describe the aircraft transponder capabilities and airborne status, may also be left unencrypted for ease of providing byte-aligned input. The Feistel split provides a balanced 52 bits for the A and B halves of the message.

The rapid transmission rate and associated controller scope refresh rate are perhaps the greatest perceived benefits of the FAA’s transition to ADS-B surveillance. Adding encryption increases the processing time at both ends of the message transmission. The pseudocode in Fig. 2 indicates that each FFX round requires two AES encryption calls, resulting in a total of 24 calls to encrypt/decrypt one message; this can contribute to costly delays in transmission. However, as we show in the following discussion, the number of AES calls can be drastically reduced.

The sole variable in the devised P string of the function F is dependent on the following tweak equation [1]:

\[ P = [1^{2}][2^{1}][0^{1}][2^{1}][104^{1}][52^{1}][12^{1}][10^{1}] \]

If the size of the tweak parameter is predetermined and static, then P is constant and enables the value of AESK(P XOR 0) to be computed once and stored as \( P' \). As a result, AESK(Q XOR P) is the only calculation that is required per round; this ultimately reduces the number of AES calls invoked per message by half. In our research, FFX was evaluated in its basic form with the tweak limited to one byte and held constant in all the tests.
5. Algorithm evaluation

The goal of encryption is to alter the plain text message in a predetermined manner, obfuscating the content by reducing the recognizable structure of the original message. This is accomplished by implementing confusion (i.e., altering the plain text in a complicated, seemingly unpredictable, manner) and diffusion (i.e., dissipating redundancies and distributing localized changes) [17,18].

Entropy is often used in cryptography to quantify the uncertainty of a bit string. It indicates the number of bits that are required to represent the given information. A truly random, and therefore unpredictable, string requires eight bits per byte to represent information regardless of any knowledge pertaining to the preceding bytes. The higher the entropy, the greater the illusion of unpredictability provided by a cryptographic scheme, which is, of course, highly desirable.

Experiments were designed to test the confusion and diffusion properties of the FFX-A2 algorithm and its ability to provide security in the ADS-B environment. Entropy was used as a measure in the tests. The ent tool [22] was used to calculate entropy.

To test the encryption algorithm, a random binary file was obtained from [16], capitalizing on the inherent unpredictability of atmospheric noise. A single pre-generated file provided enough data to generate more than 80,000 test messages (13 bytes each). A set of 20 files, each comprising 4000 test messages, were generated from the binary file for each test scenario. The set of purely random files were tested to provide a baseline for comparison.

The entropy values of the random input files and encrypted outputs are shown in Table 2. The mean entropy values of the plain text and encrypted output are 7.9965 bits per byte with little variance. This provides the standard for randomness of the input and verifies that the encryption process does not detract from the given entropy. Note that the standard deviation values in the subsequent tests were also small, yielding confidence intervals that were too small to graph.

5.1. Fixed bytes

Initial tests were designed to observe the effect of repetitive and predictable inputs on the entropy of the encrypted output. In this round of tests, 3, 6, 9 and finally 12 bytes of the 13-byte strings were held constant (i.e., repeated in every message within the file) before the result was encrypted. The fixed bytes were first inserted consecutively in the front of the message and then dispersed randomly throughout each string. In the “3 Front” test (left-hand side of Fig. 4), the first three bytes were the same in all messages within the file. On the other hand, in the “3 Random” test (right-hand side of Fig. 4), the same three bytes appear in every string, but each within a random, not necessarily consecutive, location. These tests were devised to provide insight into the diffusion properties of the algorithm.

As shown in Table 3 and Fig. 5, the entropy values of the unencrypted input files steadily decrease as expected. However, in nearly all the cases, the entropy of the encrypted output yielded 7.996 bits per byte even in the “Front” scenarios, which indicates successful diffusion across the repeated input. Note that the encryption of 12 fixed consecutive bytes (“12 Front”) yields a slight decrease (7.9407 bits per byte). In this situation, the message space was merely $2^8$, which forces the repetition of entire messages within each file. This was the first scenario that exhibited repetition, resulting in the associated decrease in the entropy of the encrypted files.

5.2. Fixed fields

The range of input data was confined to plausible ADS-B message values for the next test suite in order to observe the impact of lower entropy input. The ME field of an ADS-B message includes aircraft position information as shown in Fig. 6. The values of the altitude, geographical position and type code bits in the ME field were limited in order to represent feasible ADS-B messages. The PI field was also properly calculated, further reducing the message space and the entropy of the input messages.

5.2.1. Aircraft altitude

The altitude component of the ME field consists of 12 bits. Eleven of these bits are used to represent the numerical value of the altitude while the 12th bit indicates if the value is expressed in 25 or 100 foot increments [11]. This encoding process can represent an altitude as high as 205,800 feet, which is clearly beyond the operating parameters of traditional aircraft. Instead, this field was limited to represent likely altitudes of 20,000 to 36,000 feet. This 16,000 foot window represents a conservative view of altitudes and yields a total of 800 different representations using the encoding. Subsequently, the altitude field was forced to represent values from 0 to 799 inclusive.

5.2.2. Aircraft position

The geographical position constitutes 34 bits of the ME field and is represented using the compact position reporting (CPR) encoding. This encoding scheme was developed specifically for ADS-B messages in order to accurately represent the

| Table 2 – Results from testing unaltered random data. |
|-----------------------------------|-----|-------|
| Mean entropy (bits/byte) | 7.9965004 | 7.99642575 |
| Standard deviation | 0.000265463 | 0.000321186 |
| Confidence interval (95%) | 0.000116342 | 0.000140763 |
global position of an aircraft within about 5.1 m [13]. Given the circumference of the earth, this precision would require a minimum of 22 bits for each latitude and longitude value, but using CPR requires just 17 bits for each value. CPR establishes a dual grid-like coordinate system using 360 nautical mile (NM) square zones. Each zone is then divided into bins, approximately 5.1 m in length, in the longitudinal and latitudinal directions, which are referenced by the associated 17 bits. The identification of the corresponding bin constitutes the broadcast position. The two zone grids are slightly offset from one another and a message from each of these grid systems, “even” and “odd,” must be received within 10 s in order to validate the global position of an aircraft. Interested readers are referred to [13] for additional details; we used this information to logically limit the represented position in the tested input.

Messages received by a transceiver necessarily portray a location within its range of reception. According to [15], a receiver is required to provide a range of 120 NM, creating a circle of reception around the receiver with an equivalent radius. Fig. 7 shows the simple geometry, based on the estimate of 5.1 m per bin, that was used to determine the number of bins included in a 120 NM² portion of the zone and in the circle of reception. This yielded a truncated decimal value of 5,965,469,055 bins per grid system. Note that this is not an exact count as the circular area does not count each partial bin uniquely, which makes it a conservative estimate. The “F” bit, which indicates if the named bin is located in the “even” or “odd” system, was determined randomly. The decimal value represented by the 34 position bits (i.e., latitude and longitude) was limited to the value calculated.

5.2.3. Type code
The type code consists of the first five bits of the ME field. The code indicates the type of message that follows. This research focuses exclusively on airborne position reports for

---

### Table 3 – Results from testing fixed bytes input files.

<table>
<thead>
<tr>
<th>Location</th>
<th>Plain text</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front 3 Bytes</td>
<td>7.2402034</td>
<td>7.9964316</td>
</tr>
<tr>
<td>Random 3 Bytes</td>
<td>7.24026595</td>
<td>7.9964776</td>
</tr>
<tr>
<td>Front 6 Bytes</td>
<td>6.40927475</td>
<td>7.9965103</td>
</tr>
<tr>
<td>Random 6 Bytes</td>
<td>6.4092798</td>
<td>7.9964106</td>
</tr>
<tr>
<td>Front 9 Bytes</td>
<td>5.44052755</td>
<td>7.99638325</td>
</tr>
<tr>
<td>Random 9 Bytes</td>
<td>5.44106955</td>
<td>7.9965158</td>
</tr>
<tr>
<td>Front 12 Bytes</td>
<td>4.2479117</td>
<td>7.9407372</td>
</tr>
<tr>
<td>Random 12 Bytes</td>
<td>4.2473267</td>
<td>7.9964125</td>
</tr>
</tbody>
</table>

---

![Fig. 4 – Sample input messages for the three fixed bytes test.](image)

![Fig. 5 – Measured entropy (mean) for the fixed bits tests.](image)

![Fig. 6 – Bits in the ME field.](image)
which there are only 14 associated type code values (0, 9–18, 20–22) [15]. The values of the type code bits were equivalently limited.

5.2.4. Parity/identity field
The PI field is calculated as a cyclic redundancy check, depending on the preceding 88 message bits and the following polynomial [12]:

\[ G(x) = 1 + x^1 + x^{10} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24}. \]

As mentioned above, the first byte of an ADS-B message contains the DF and CA fields, which remain unencrypted to meet system functionality requirements. For the purposes of the fixed fields tests, the DF and CA fields were assumed to represent the values of 10001 and 101, respectively (i.e., 8D in hexadecimal), and were included in the calculation of the associated parity. While the three bytes resulting from the PI calculation obviously vary, they do so in a prescribed manner, thereby affecting the message entropy.

5.2.5. Entropy assessment
The original random input was altered based on the parameters discussed above to create representative ADS-B messages. However, true ADS messages are not only logically limited, but also contain fields (e.g., aircraft address) that are constant for all subsequent message transmissions. Therefore, the number of message fields held constant in each file was increased. This scenario represents a worst case and is indicative of an adversary conducting a “known plain text” attack.

The represented position (34 bits) was the first field held constant, followed by the altitude (12 bits), aircraft address (24 bits) and finally the type code (5 bits). In all instances, the proper message parity was calculated. The tests were conducted in a cumulative manner such that the input for the final test case included all four fixed fields, forcing a total of 75 out of 104 bits to be constant in each input file. Note that this final test case resulted in only the five bits associated with “S,” “T” and “F” as random fields, with the remaining 24 bits derived from the calculated parity.

The results of the fixed field tests are shown in Table 4 and Fig. 8. The entropy of the plain text files steadily decreased as the number of fixed fields increased, similar to the results in the fixed bytes test. The measured entropy for the encrypted output was again 7.996 bits per byte for the cases with zero, one, and two fixed fields. Note the slight drop in the measured entropy for three fixed fields. The four fixed fields test yielded the lowest entropy. In the case of the three and four fixed fields tests, message repetition was assured because the associated message spaces were just $2^{10}$ and $2^5$, respectively.

While the fixed field tests more accurately reflect the ADS-B environment, they do not represent true operational use. Successive messages originating from the same aircraft exhibit minimal differences during flight. Indeed, the configuration bits remain constant while the position field values demonstrate gradual changes associated with aircraft latitude, longitude and altitude.

5.3. Aircraft traffic
The final test involved the use of position information generated from actual aircraft traffic. An aircraft track shown in Fig. 9, as observed by traditional radar sources, was obtained from the Western Air Defense Sector. The Western Air Defense Sector reports to the North American Aerospace Defense Command (NORAD) and continually monitors the U.S. airspace to ensure air sovereignty and strategic air defense. As seen in Fig. 9, the aircraft took off from Oakland, California before traveling eastward toward Nebraska. The provided track includes altitude and position information from overlapping radars with updates every 1–7 s, yielding small variances between successive points.

The positions were transformed into ADS-B messages using the “Message Generator” code produced in [11]. In totality, the track included more than 4400 positions from

![Fig. 7 – Geometry used to calculate the number of bins (viable positions) in a standard reception area.](image)

<table>
<thead>
<tr>
<th>Fixed fields</th>
<th>#Bits</th>
<th>Plain text</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random (none)</td>
<td>0</td>
<td>7.94772295</td>
<td>7.9964494</td>
</tr>
<tr>
<td>Position</td>
<td>34</td>
<td>6.9046341</td>
<td>7.9964559</td>
</tr>
<tr>
<td>Position, altitude</td>
<td>46</td>
<td>6.5156282</td>
<td>7.9964274</td>
</tr>
<tr>
<td>Position, altitude, address</td>
<td>70</td>
<td>5.55284515</td>
<td>7.9638198</td>
</tr>
<tr>
<td>Position, altitude, address, type code</td>
<td>75</td>
<td>5.0601405</td>
<td>7.4906553</td>
</tr>
</tbody>
</table>

Table 4 – Mean entropy results from the fixed field tests.
which the “even” and “odd” CPR position messages were generated. Unlike the previous tests, the messages in this test file were guaranteed to be unique. The entropy of the plain text messages was measured at 6.513979 bits per byte while the encrypted output yielded an entropy of 7.998633 bits per byte. These results are consistent with the findings of the fixed bytes and fixed fields tests. In fact, the encrypted entropy from the actual track is higher than that resulting from any test dependent on the pre-generated random file obtained from [16]. These findings support the ability of the FFX algorithm to adequately confuse and diffuse the message content of ADS-B aircraft position messages.

6. Conclusions

The experimental results presented in this paper suggest that a subset of the FFX-A2 algorithm is suitable for encrypting ADS-B messages, and provides sufficient diffusion and confusion to obfuscate inherently redundant message fields. Even with 12 of the 13 message bytes fixed, the entropy of the encrypted output indicates that the algorithm effectively obfuscates message content.

While the findings indicate that the FFX algorithm may be used to provide ADS-B message security, key management is an issue that remains to be addressed. Our future research
will attempt to implement a secure controller-pilot communication data link for communications between the pilot and air traffic control. This may enable out-of-band key transmission and provide a means for network-wide implementation. While exhaustive evaluations of the FFX algorithm are still being conducted, the results of this paper indicate that the algorithm has the potential to be employed in the ADS-B system to provide message confidentiality for aircraft surveillance.

Acknowledgments

Note that the views expressed in this paper are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Department of Defense or the U.S. Government.

References