Can Cryptography Secure Next Generation Air Traffic Surveillance?

Kyle D. Wesson, *Student Member, IEEE,* Todd E. Humphreys, *Member, IEEE,* and Brian L. Evans, *Fellow, IEEE*

***Abstract*—The proposed next-generation air traffic control system depends crucially on a surveillance technology called ADS-B. By 2020, nearly all aircraft flying through U.S. airspace must carry ADS-B transponders to continuously transmit their precise real-time location and velocity to ground-based air traffic control and to other *en route* aircraft. Surprisingly, the ADS-B protocol has no built-in security mechanisms, which renders ADS-B systems vulnerable to a wide range of malicious attacks. Herein, we address the question "can cryptography secure ADS-B?"—in other words, is there a practical and effective cryptographic solution that can be retrofit to the existing ADS-B system and enhance the security of this critical aviation technology?**

I. Introduction

THE year 2020 marks the dawn of aviation modernization. By that year, nearly all aircraft flying through U.S. airspace must carry Automatic Dependent Surveillance Broadcast (ADS-B) equipment, according to the Federal Aviation Administration's timeline to implement the Next Generation Air Transportation System (NextGen). ADS-B is central to NextGen, which shifts the burden of surveillance from antiquated ground-based radar to modern satellite-navigation-based aircraft transponders. Benefits of ADS-B include increased situational awareness, extended surveillance coverage, enhanced conflict detection, reduced operational costs, and improved routing efficiency [1].

Unfortunately, ADS-B as currently designed is riddled with security vulnerabilities [2]–[4]. ADS-B messages are broadcast in-the-clear according to an open protocol without cryptographic security mechanisms such as encryption or digital signatures that could protect and authenticate them. An open-access protocol has merits for international interoperability but renders ADS-B vulnerable to problems stemming from a lack of confidentiality, such as aircraft targeting for electronic or kinetic attack, and malicious injection attacks, such as displaying ghost aircraft on cockpit displays.

Proposed cryptographic solutions attempt to mitigate these vulnerabilities [5]–[7]. These proposals merit evaluation in the context of the technologically-complex, cost-averse, and interoperability-focused aviation community. To this end, we address the question "can cryptography secure ADS-B within the constraints of the proposed NextGen system?" Our holistic evaluation considers the historical design and policy constraints that shaped ADS-B, discusses the effectiveness of various candidate cryptographic solutions, and analyzes their implementation burden. We conclude with a quantitative assessment of the technological burden required to implement the most feasible cryptographic solution.

II. The Shift from Independent to Dependent Surveillance

Radar, developed in the 1940s, is the current state-of-the-art air traffic surveillance system. Primary surveillance radar (PSR) is considered an independent and non-cooperative surveillance system—independent because the radar on its own is sufficient to determine the necessary surveillance data (i.e., range and azimuth to target), and non-cooperative because the aircraft provides no assistance besides offering its cross-sectional area as a radar-reflective surface. Drawbacks of PSR include its need to perform several radar sweeps of each target, measurement accuracy that degrades with increased target range, and susceptibility to so-called clutter interference.

Secondary surveillance radar (SSR) is independent and cooperative. Like PSR, SSR determines range and azimuth from radar sweeps, but SSR additionally interrogates aircraft equipped with Mode-S(elect) beacons at 1030 MHz. The cooperative responses from an aircraft's beacon transponder at 1090 MHz augment radar-derived surveillance with the aircraft's altitude and identity from Mode-C(ontract) and Mode-A(ddress) transmissions, respectively. Not all aircraft carry Mode-S transponders; for those that do not, non-cooperative radar and voice communication are the primary surveillance technologies.

The combined U.S. PSR–SSR network provides aircraft position accuracy of 1–2 nmi with updates every 5–10 s, which leads to a 3 nmi or greater separation requirement between aircraft in most U.S. airspace under FAA Order 7110.65. The current system has been sufficient to handle past and present air traffic densities, but it cannot support the high aircraft densities that are predicted. The combination of this fact with the high operating costs of PSR–SSR systems motivate the transition from radar to the modernized ADS-B system, which will provide an accurate, real-time view of air traffic purportedly at a lower cost than radar.

The acronym ADS-B conveys how the protocol operates. ADS-B transponders *automatically* broadcast without external interrogation or pilot input. The navigation data and its quality are *dependent* on the sensors installed on board the aircraft. The message contains *surveillance* data that is *broadcast* so

K. Wesson was supported in part by DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate Fellowship 32 CFR § 168a, and The University of Texas at Austin Microelectronics and Computer Development Fellowship.

Authors are with the Wireless Networking and Communications Group, Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712 USA (e-mail: kyle.wesson@utexas.edu, todd.humphreys@mail.utexas.edu, bevans@ece.utexas.edu).

that anyone may receive it and no reply is sought. ADS-B offers position accuracy of 92.6 m (0.05 nmi), velocity accuracy of 10 m/s (19.4 nmi/h), and updates every second. These performance standards are designed to support (a) reduction in aircraft lateral separation from 90 nmi to 20 nmi and reduction in aircraft longitudinal separation from 80 nmi to 5 nmi in airspace that is outside of radar range, and (b) expansion of the 3 nmi aircraft separation requirements to airspace that currently sets a minimum 5 nmi separation [8].

When ADS-B was developed as an extension to the Mode-S beacon radar surveillance system in the 1980–90s, performance concerns focused on reliability, accuracy, range, operational capacity, and channel occupancy [9]. Note the omission of security—a topic that has received scant coverage in publicly-available reports from the FAA and other stakeholders. In response to concerns about ADS-B vulnerabilities, the FAA conducted a Security Certification and Accreditation Procedures (SCAP) study that, to date, remains protected from public disclosure because of its status as “Sensitive Security Information.” Unable to discuss their test procedures or results, the FAA instead stated in 2009 that “using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today” [8].

The FAA has committed to an annual review of its security study to evaluate new and evolving threats against ADS-B. One evolving threat targets the Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS), from which ADS-B derives its surveillance data. GPS is vulnerable to denial-of-service and signal counterfeiting attacks known as jamming and spoofing, respectively. GPS security has recently been the focus of vigorous research [10]. In 2012, the FAA tasked the “GNSS Intentional Interference and Spoofing Study Team” to evaluate the threat. Like the ADS-B SCAP study, their findings have yet to be released to the public.

At first glance, the FAA’s claim of no increased risk seems implausible given the ease with which ADS-B can be spoofed and jammed in comparison to radar. Consider the difficulty facing an attacker who wishes to fool, or spoof, SSR. For one, the highly-directional SSR beam pattern makes it difficult for the attacker to inject a false target with an arbitrary bearing or altitude. The commonplace ASR-11 surveillance radar has a 5° elevation and 1.4° azimuth beamwidth. An attacker would either need to be within this narrow beam or would have to resort to injecting its signals through the antenna’s side lobes, which would require high power or close proximity. For example, an attacker outside the main SSR radar antenna beam at a standoff distance of 1 km would need to transmit an 80 W signal, assuming a minimum 34 dBi sidelobe suppression, to match the received signal power of a 200 W Mode-S transponder at a range of 80 km. Furthermore, because radar is triggered, an attacker would need to detect when a radar pulse is sent and respond with an appropriately-timed response. Although these technical hurdles can be cleared, they increase the cost of an attack and limit its scale. Unsurprisingly, radar spoofing and jamming attacks “very rarely occur” [8].

By way of comparison, consider an attack against ADS-B. Omnidirectional ADS-B antennas afford attackers flexibility in orientation and proximity. The power from a 125 W ADS-B transceiver 80 km away is matched by a 20 mW transmitter 1 km away. Forged ADS-B message broadcasts can initiate anytime and can continue at 1 Hz, commensurate with the ADS-B transmission rate. Couple this relative physical flexibility with the lack of built-in security mechanisms, and it becomes clear just how vulnerable ADS-B is: a single, fraudulent, properly-formatted ADS-B transmission that passes parity is indistinguishable from an authentic message from the point-of-view of an ADS-B receiver.

Even so, the FAA’s original claim regarding risk may not be inaccurate. In response to concerns about spoofing and jamming attacks against ADS-B or GPS, the FAA plans to retain near legacy levels of radar as a backup for ADS-B surveillance. The agency will continue to operate 100% of the 150 *en route* SSRs and will retain 40 legacy SSRs, or approximately 50%, in some high-density areas [8]. Class B airports—those with the highest air traffic density in the U.S.—will retain legacy-level coverage. By maintaining these radar systems, the FAA will not reap the cost-savings originally predicted from NextGen until after 2035, but air traffic control (ATC) will retain the ability to cross validate ADS-B broadcasts with radar, thereby providing near-legacy-level surveillance security.

There are good reasons, however, to demand *better* than legacy security. As with ADS-B, worrisome weaknesses also exist in the legacy air traffic surveillance system: Mode-S, A, and C have no cryptographic safeguards, and voice communication over radio between ATC and pilots is unencrypted. Legacy surveillance systems also operate with aircraft separation requirements that NextGen will reduce in some airspace. If ADS-B is working as intended, the tighter spacing is likely no less safe than legacy spacing, but if an attack occurs, tighter spacing will increase the chance of a mishap. Under attack, legacy-level security cannot maintain legacy-level risk.

Besides, legacy-level security appears oddly out-of-date in a post-9/11 world. After the 9/11 attacks, the FAA oversaw the installation of reinforced cockpit doors, and air-bound passengers continue to endure enhanced screening procedures administered by the Transportation Safety Administration. Why then should NextGen be content with legacy-level security? The modern aviation risk landscape has also been altered by new technology. Whatever security concerns may have arisen during ADS-B development in the 1990s were likely assuaged by the high costs of acquiring ADS-B hardware and mounting a successful attack. Four decades later, a do-it-yourself ADS-B transponder that can produce counterfeit ADS-B messages can be made for just $1,000 [4]. Greater risk calls for greater security. Thus, even if the FAA’s claim of no increased risk is accurate, there remain good reasons to pursue a cryptographic fix for ADS-B.

III. The Technical Ins and Outs of ADS-B

The following technical details will aid understanding of the security problems and the constraints of the ADS-B protocol. ADS-B Out messages are broadcast every second at a data rate of 1 Mbps over either 1090 MHz Mode-S Extended Squitter

(ES) or 978 MHz Universal Access Transceiver (UAT) [1]. This dual-link strategy is a compromise that the FAA made to satisfy international standards that require 1090 MHz Mode-S ES and those general aviation pilots who have already purchased UAT transceivers. Despite its name, UAT is a U.S.-only protocol for general aviation aircraft flying below Class A airspace, which begins at 18,000 ft, and outside of other controlled airspace, such as Class B airspace.

To support aircraft equipped with an ADS-B transponder that only operates at one frequency, the FAA will install ADS-R(ebroadcast) capabilities in ADS-B ground stations to rebroadcast Mode-S ES messages in UAT format and *vice versa* [8]. Each ADS-R system will have a range of 150–200 nmi, and the costs of installing and running the network will be borne by the FAA. To ensure ADS-R stations can receive ADS-B messages with sufficient power, the FAA has set the minimum transmission power of ADS-B at 125 W for 1090 MHz Mode-S ES broadcasts.

ADS-B Out messages are modulated with pulse position modulation (PPM), which is a type of pulse amplitude modulation (PAM). Differential phase shift keying (DPSK) was also considered. DPSK has a lower bit error rate than PAM for a given signal-to-noise ratio but had a higher hardware cost. Designers selected PPM to minimize costs and maintain interoperability—that is, the compatibility of ADS-B with existing protocols and equipped hardware.

ADS-B Out messages are 112-bits long. The first 8 bits indicate the data format, the next 24 bits indicate the aircraft's unique and fixed International Civil Aviation Organization (ICAO) address, the next 56 bits transmit the ADS-B surveillance data, and the final 24 bits are a cyclic redundancy check block. During flight, an aircraft's 112-bit ADS-B Out Data Format 17 messages contain the time and the aircraft's latitude, longitude, and altitude. Other 112-bit message formats are broadcast to communicate other operational events when the aircraft is on the tarmac.

The FAA only requires equipage of ADS-B Out by 2020; ADS-B In remains optional because of concerns regarding its implementation cost, equipment performance standards, and cockpit display requirements. Nonetheless, complete ADS-B In/Out systems will be popular because of the additional situational awareness, more efficient oceanic routing, and enhanced aircraft interval management that ADS-B In/Out offers over ADS-B Out alone. Figure 1 illustrates a basic operational ADS-B system.

No part of the ADS-B Out messages is encrypted or cryptographically signed. The lack of cryptographic safeguards is likely explained by the original designers' focus on interoperability, a principle that is evident throughout the design of ADS-B. Its frequencies, 1030 MHz interrogations and 1090 MHz responses, allow Mode-S and ATC to communicate over the same channel; its modulation scheme, PPM, was supported by existing, low-cost hardware in the 1990s; and its short message length, 112 bits, was an attempt to minimize communication interference with existing protocols. Interoperability facilitates adoption and keeps cost low, whereas cryptographic techniques limit international adoption and increase costs. When viewed in the context of interoperability, ADS-B is a well-designed open-access protocol.

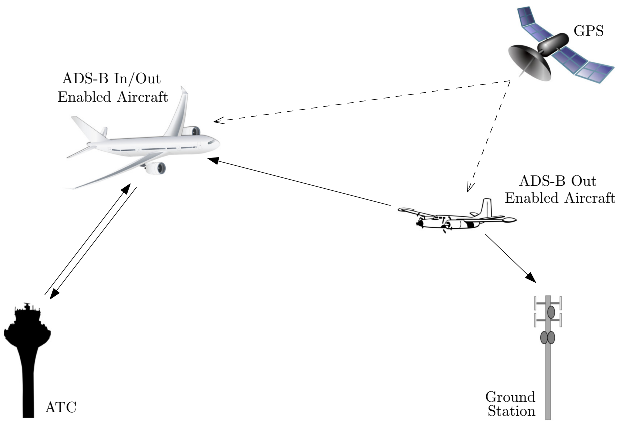

Fig. 1. An overview of the ADS-B system, adapted from [1]. Aircraft are only mandated to broadcast ADS-B Out messages; receipt of ADS-B In messages is optional. Radar and other aviation broadcast messages are not shown.

IV. Concerning Scenarios

Consider the following scenario: *Suppose a pilot wishes to fly in secret. During flight, the ADS-B transponder continuously broadcasts ADS-B messages that contain the aircraft's unique identifying number and real-time position. A network of ADS-B receivers operated by aviation enthusiasts throughout the country tracks all aircraft, including his, in real-time, and publishes the data online.*

In response to privacy concerns voiced by the aviation community, the FAA stated that "there is no right to privacy when operating in the [National Air Space]" [8]. Aircraft flying through Class A, B, C, D, and E airspace must identify themselves to ATC during flight under 14 CFR § 91.215 regulations. However, the FAA does suggest a way to fly anonymously: pilots who choose to employ a UAT-equipped transceiver operating in pseudo-anonymity mode under visual flight rules can maintain anonymity if they do not file a flight plan and make no use of ATC services. In the U.S., this scenario is possible only in Class G airspace. Thus, anonymity remains elusive for aircraft equipped with 1090 MHz Mode-S ES transponders or for aircraft that fly through ATC controlled airspace.

While it is true that aircraft using public airports cannot expect privacy—a pair of binoculars will fare just as well as an ADS-B tracking system—the automation of ADS-B offers a far easier and more persistent way to track an aircraft than does manual surveillance. Such an automatic tracking capability presents an array of concerns similar to those that the U.S. Supreme Court faced in its 2012 ruling on GPS monitoring under the Fourth Amendment in *United States v. Jones*. The Court's 2012 ruling notes the striking difference between conventional and automatic surveillance, of which ADS-B is another example.

Beyond the concerns over the persistence of ADS-B tracking are concerns about its immediacy. Many flight tracking websites display information obtained from the Aircraft Situational Display to Industry (ASDI) that the FAA has offered to a variety of clients since 1998. While ASDI data is offered in real-time to commercial airline companies and flight management companies, most others receive ASDI with at least a five minute delay. The delay was implemented in response to the attacks of 9/11. With ADS-B, however, precise positions and velocities transmitted in real-time are accessible to anyone with an ADS-B receiver. A worrisome possibility of which the FAA is aware is one where real-time, in-the-clear ADS-B broadcasts are used to target passenger aircraft for kinetic or electronic attack [8].

Leaving privacy aside, consider the following scenario: *A rogue hobbyist living near a major airport decides to build a software-defined ADS-B transponder capable of broadcasting forged ADS-B messages. She programs the transponder to broadcast the positions of hundreds of counterfeit aircraft surrounding the airport. Some of these counterfeit positions are close enough to the actual aircraft that other surveillance techniques such as multilateration, angle-of-arrival discrimination, or radar scans cannot distinguish between the legitimate and forged aircraft. ATC and pilots respond by reverting to radar and voice, thereby vitiating the efficiency gains of ADS-B. A plane crash-lands when false aircraft trajectories and low-visibility conditions cause confusion in the cockpit.*

Attacks against ADS-B, such as the one in the preceding scenario as well as those listed in Table I, can confuse pilots and ATC. Confusion is not deadly on its own, but when it is coupled with a stressful situation, such as takeoff or landing, or with compounding conditions, such as snow or wind, the results can be lethal. Recent events including the 2013 crash of Asiana Airlines Flight 214 have indicated a decline in airmanship in favor of technological reliance. How will pilots who have become increasingly reliant on an autopilot and GPS fare when faced with spoofed but plausible ADS-B messages?

V. Cryptography for ADS-B

In this section, our goal is to address the question “can cryptography secure ADS-B within the constraints of the current system?” In the discussion that follows, we evaluate proposed ADS-B cryptographic strategies based on their practicality and effectiveness in the technologically-complex, cost-averse, and interoperability-focused aviation community. Each proposal falls into one of four categories: symmetric-key encryption, message authentication codes, asymmetric-key encryption, or digital signatures.

Retrofitting a cryptographic technique to the existing ADS-B protocol faces many difficulties:

- ADS-B is an international protocol. A cryptographic solution must harmonize with existing policy, such as export control laws, and technological capabilities.
- ADS-B is bandwidth constrained. Additional spectrum for ADS-B is scarce, and existing spectrum allocations may actually shrink (c.f., [1], Appendix F).
- ADS-B is interference constrained—that is, the number of aircraft that the ADS-B system can support is limited by interference in the Mode-S ES and UAT frequency bands. Extending the ADS-B message length will increase interference and reduce operational capacity.
- ADS-B operates in a cryptographically untrusted environment. Whatever cryptographic hardware, software, and keys are ultimately employed will be accessible to malicious parties.

The following discussion focuses on the ADS-B 1090 MHz Mode-S ES because of the limited operational scope of UAT. We outline a variety of proposed cryptographic enhancements to ADS-B, postponing until the next section a determination and discussion of the most feasible option.

A. Symmetric-Key Cryptography

Symmetric-key techniques are known to be computationally efficient. The premise of these techniques is that the sender and recipient share a secret cryptographic key. Without knowledge of the shared secret key, the encrypted messages and message authentication codes (MACs) generated via symmetric-key algorithms are computationally infeasible to forge or predict. In addition, the secret key cannot be derived from the encrypted messages known as the ciphertext.

1) Symmetric-Key Encryption: Encrypting ADS-B messages via symmetric-key methods means (a) selecting an appropriate symmetric-key encryption algorithm (e.g., Advanced Encryption Standard [AES] or Triple Data Encryption Algorithm), (b) computing and disseminating a cryptographic secret key, and (c) broadcasting the encrypted ADS-B messages in place of the unencrypted, or plaintext, ADS-B messages. A byproduct of symmetric-key encryption is confidentiality: the encrypted message is unintelligible to those without knowledge of the secret key.

In the spectrum- and interference-constrained ADS-B system, a standout symmetric-key encryption protocol is format-preserving encryption (FPE), because the plaintext and resulting ciphertext are the same length. FPE also allows certain ADS-B message parameters to remain unencrypted, such as the data format field, which would facilitate interpretation [11]. Still, FPE remains under review at the U.S. National Institute of Standards and Technology (NIST), and despite favorable early reviews, FPE is not standardized. Other standardized, length-preserving alternatives are feasible, such as AES running output feedback mode with an 8-bit block size. Our subsequent analysis, however, finds that no matter how appealing format-preserving protocols may be, symmetric-key encryption is impractical.

2) Symmetric-Key Message Authentication Codes: MACs are typically short messages that are derived from a longer message based on specific MAC-generating algorithms (e.g., keyed-hash message authentication code or parallelizable MAC). The MAC is generally appended to the longer message and the message–MAC pair is broadcast together to allow for immediate validation. A successful verification of the message–MAC pair ensures the recipient that the message–MAC pair were not manipulated after the MAC was generated. However, a MAC approach does not provide confidentiality, because the plaintext is still broadcast.

MACs would increase the message length and would thereby increase the potential of ADS-B message interference, or overlap, during broadcast. Supporting MAC-induced

Attack	Description	Potential Ramifications
Interception	ADS-B Out messages can be decoded by any ADS-B receiver within range	Loss of privacy; persistent monitoring; targeting for kinetic or electronic attack
Jamming	A jammer can disrupt legitimate ADS-B message reception	Denial of service; fallback to older, less efficient technologies
False Injection	ADS-B messages can be forged and broadcast with intent to deceive air traffic control and aircraft	Falsely indicate a collision appears imminent; confuse pilots or ATC; interfere with legitimate message reception
Navigation	Satellite navigation systems (e.g., GPS) can be spoofed or jammed	False ADS-B position or velocity information; fallback to radar or voice communications

TABLE I
THERE ARE A VARIETY OF ATTACKS THAT CAN TARGET ADS-B AND THE SERVICES FROM WHICH IT DERIVES ITS SURVEILLANCE DATA. SOME OF THESE ATTACKS CAN BE FOUND IN [2]–[4], [10].

interference on the 1090 MHz channel could vitiate the gains of ADS-B by reducing the system's operational capacity. A potential alternative broadcast scheme is a "lightweight" approach: instead of broadcasting the message–MAC pair together, one transmits only portions of the MAC with every message [3]. The portioned MAC bits could be appended to regular ADS-B messages or broadcast over spare bits in alternate message formats [5]. The downside of the lightweight approach is that it introduces a delay between transmission of the original ADS-B message and the message's eventual MAC-based verification. The next section quantitatively discusses this interference tradeoff.

3) Symmetric Key Management: Symmetric-key techniques suffer from a serious drawback. Any party with knowledge of the secret key can generate a message that will pass cryptographic validation. This means that a single secret key leak compromises the entire system. The security of a symmetric-key system, therefore, depends crucially on the security of the secret key which is required for both encryption and decryption operations as well as MAC generation and validation. To support ADS-B, the secret key must be accessible to every ADS-B transceiver. Secret keys have a short lifetime when they are distributed among potentially untrustworthy groups. Consider that the Sony PlayStation 3 secret key was discovered only two years after its retail debut despite the intentions of system engineers to prevent a key leak.

Three secret key distribution strategies have been proposed: (1) distribute keys to all aircraft in tamper-proof hardware, (2) distribute keys only to select aircraft in tamper-proof hardware, or (3) distribute keys on a per-flight basis via air traffic control during preflight operations. The first approach remains vulnerable to the single-key disclosure leak problem and hinges on the security of the tamper-proof equipment. The feasibility of the second approach, while favored in [11] for civil and military applications, is questionable. How will these "secured" users interact with the "unsecured" users? Is a private-key-holding aircraft supposed to ignore unverifiable messages? What happens if valid yet unverifiable messages are ignored?

The third proposed approach is to distribute a unique secret key for every aircraft on a per-flight basis [5], [7]. During preflight, air traffic control could assign keys that are valid for only that flight and enter those keys into an international database to assist in interactions with other aircraft. The drawback of this approach is that the symmetric key must be securely distributed to every other agent who needs to validate the messages, and those users could, in turn, impersonate the intended user or leak the key. The approach is also vulnerable to a leak of the entire active key database.

B. Asymmetric-Key Cryptography

Asymmetric-key cryptographic techniques, while less computationally efficient and less length efficient than symmetric-key techniques, can be as secure as their symmetric-key counterparts. Asymmetric-key approaches distribute public–private key pairs via a public-key infrastructure (PKI) where every user has a public–private key pair bound to their identity by a Certificate Authority (CA). The FAA or ICAO could assume the role of CA.

Asymmetric-key techniques have an important advantage over symmetric-key techniques: Alice cannot forge Bob's asymmetric-key encrypted or signed message with her own private–public key pair. So, if a private key is compromised, then only a single key pair needs to be revoked. This stands in contrast to the symmetric-key approach where a single key leak renders the entire system compromised. A PKI has provisions for revoking compromised keys.

1) Asymmetric-Key Encryption: In an asymmetric-key encryption paradigm, users would encrypt the ADS-B message with the intended recipient's public key according to a specific public-key encryption technique (e.g., elliptic curve cryptography [ECC]). The recipient could then decrypt the message with his or her own private key. Confidentiality is also a byproduct of asymmetric-key encryption because only the sender's intended recipient can decrypt the transmission.

Asymmetric-key ADS-B message encryption has two significant drawbacks. First, asymmetric-key block or stream ciphers would increase the transmitted ADS-B message length, much like MACs. Second, and more problematically, unique encrypted ADS-B messages would be required for each recipient [7]. To maintain a fully-connected network of n aircraft would necessitate $(n^2 - n)$ unique broadcasts rather than n in the current system.

2) Digital Signatures: Digital signatures are similar to MACs in the sense that they are appended to the original in-the-clear ADS-B message. Digital signature algorithms (e.g., *the* digital signature algorithm [DSA] or elliptic curve DSA [ECDSA]) take a message and a user's private key as input and return a digital signature unique to the input. Upon reception of the message–signature pair, or signed message, the recipient can apply a verification algorithm that authenticates the signed message with the sender's public key. A successful authentication means that the signed message originated with the sender and was not modified *en route*. Digital signatures could be transmitted in the same ways discussed earlier for MACs.

Within the family of digital signature algorithms, ECDSA generates the shortest digital signatures for a given equivalent symmetric-key security level, which makes ECDSA enticing for ADS-B when coupled with a PKI standard such as the International Telecommunications Union (ITU) X.509 standard [12], [13]. For a symmetric-key equivalent strength of 112 bits, which NIST claims is cryptographically secure until 2030, the ECDSA signature length is 448 bits. Note that this signature length is four times greater than the length of an ADS-B message.

3) Key Management: Public keys are public, like the name suggests, whereas private keys must remain secret to protect the security of the system. Asymmetric techniques can leverage a PKI to generate, disseminate, and revoke keys [13]. Before flight, a complete list of all known public keys or a list of those that had changed since the last flight could be uploaded to the aircraft. Real-time key creation and revocation could be communicated over satellite or ground data links that are available on most commercial flights.

VI. Can Cryptography Secure ADS-B?

The previous section outlined four cryptographic ADS-B enhancements that were proposed to secure ADS-B. Yet a host of real-world considerations and practicalities mean that only one of these techniques is remotely practical.

First, consider encryption. One of the FAA's goals is to ensure international operation of ADS-B. While the FAA appears to have no policy that explicitly prohibits encryption on civil aviation protocols, the agency states that requiring encrypted ADS-B messages would "unnecessarily limit [ADS-B] use internationally" [8]. Even if the problem of international interoperability could be overcome, one suspects that the FAA and ICAO would reject ADS-B encryption because it undermines traditional safety: Legitimate but encrypted ADS-B messages may at times not be decryptable either due to a technical failure or human error, increasing the risk of aircraft collisions. It is extremely unlikely that the FAA or ICAO would trade this obvious increased risk for a reduction of the hypothetical risks associated with open-access real-time ADS-B broadcasts. Thus, we believe, ADS-B encryption is not viable.

It is worth pausing to consider the implications of this claim. Without ADS-B encryption, pilots of ADS-B–equipped aircraft who do not wish their aircraft's real-time precise position and velocity to be broadcast publicly to the curious and to the malign will have only one option in U.S. airspace: don't fly.

Next, consider symmetric-key techniques. Contrary to [3] and [11], we believe that the threat of symmetric-key leaks and the burden of key management renders symmetric-key encryption and MACs entirely impractical. It is unlikely that the FAA or ICAO would be willing to accept the risk of a symmetric key leak and the subsequent burden of securely re-keying every aircraft worldwide.

Therefore, of the four options discussed previously, asymmetric-key digital signatures are the only viable cryptographic enhancement for ADS-B within the constraints of NextGen. Among the possible digital signature algorithms, ECDSA generates the shortest digital signatures for a given key strength, making it the most appropriate choice in a bandwidth- and interference-constrained communication channel. To further investigate the practicality of an ECDSA-based ADS-B solution, we analyze the PKI and interference burden of its implementation.

A. Public Key Infrastructure Burden

To enable digital signatures, the aviation community would need to embrace a PKI infrastructure to handle public–private key creation, assignment, and revocation. The ITU X.509 standard, already implemented in non-aviation applications, specifies certificate formats, attributes, and algorithms to facilitate PKI. The authors of [12] and [13] propose X.509 to support cryptographic enhancements to ADS-B. A possible conduit for ground-to-plane data transfer of key certificates and revocation lists is the Airplane Asset Distribution System (AADS), which provides a framework and a nomenclature for aviation security. The authors of [13] propose AADS to support aviation security.

While feasible, PKI would be a significant financial and technical burden on the aviation community. This burden includes distributing public keys to aircraft and ground control, securing private keys during transmission and operation, and implementing real-time key revocation. A Verisign-like entity with experience in global PKI management is likely better suited for the task than either the FAA or ICAO.

According to FAA, there were approximately 225,000 general aviation aircraft and 7,500 commercial aircraft in the U.S. in 2011. Each wishing to use ADS-B would need a public–private key and would need to securely store the private key. To verify signatures, each plane would also need a list of all other public keys. Assuming the maximum size of a X.509 certificate is about 5 kB, then the size of the full U.S. public–private key database would be about 1.2 GB.

Real-time revocation remains a significant challenge as voice channels are not designed to support revocation. AADS as described in [13] is proposed for communication with aircraft on the ground and would need to be adapted to communicate with aircraft in flight. Another possibility would be to revoke keys over the Flight Information Services Bulletin (FIS-B), which is designed to communicate temporary flight restrictions and airspace information. However, FIS-B is broadcast over UAT frequencies, meaning that aircraft equipped with 1090 MHz Mode-S ES transponders cannot receive FIS-B without additional hardware. General aviation is unlikely to equip even more technology to support cryptographic enhancements to ADS-B alone, and the FAA is sensitive to its own costs as well as those costs borne by the aviation community. Recall that costs were a driving factor for the dual-link ADS-B strategy.

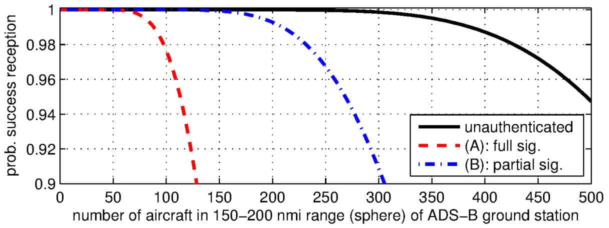

Fig. 2. Plot showing air traffic operational capacity within a 150–200 nmi range (sphere) of an ADS-B ground station with the addition of ECDSA signatures as compared to unauthenticated broadcasts in the 1090 MHz Mode-S ES band. The red dashed line corresponds to scenario (A): a 560 bit signed message consisting of a 112 bit ADS-B message and its 448 bit signature. The blue dot-dashed line corresponds to scenario (B): a sequence of nine 112 bit messages where the first is the standard ADS-B message and the rest are 56-bit segments of the ECDSA signature packaged in the ADS-B framing structure.

B. Interference Burden

If the ECDSA signature is broadcast over 1090 MHz Mode-S ES, it will increase interference and reduce the number of aircraft that ATC can support. Here, we estimate the resulting reduction in operational capacity based on the operational scenarios presented in earlier ADS-B capacity analysis [9], [14].

The ECDSA signature length is 448 bits for a symmetric-key equivalent strength of 112 bits. Two possible broadcast scenarios were analyzed: (A) the broadcast of a 560-bit signed message consisting of a 112-bit ADS-B message and its 448 bit signature, and (B) the broadcast of a sequence of nine 112 bit messages where the first is the standard ADS-B message and the subsequent eight are 56-bit segments of the ECDSA signature packaged in the ADS-B framing structure. The former scenario assumes, optimistically, that the ADS-B message format could be altered, while the latter scenario assumes that the signature can be inserted into the 112 bit ADS-B message format in place of surveillance data but that the 112-bit ADS-B message structure is unchangeable.

The estimate of air traffic operational capacity is based on several assumptions from [14]. The model assumes that the probability distribution of message receipt times over the 1090 MHz channel is Poisson with rates proportional to the "moderately high" interference scenario in [9]. The model further assumes that only one interference message overlap can be tolerated per received message. Lastly, it assumes that aircraft employ a single bottom mounted 125 W antenna to transmit ADS-B messages [8]. Although reducing the transmit power would address the interference problem by reducing the range of receipt of ADS-B messages, the 125 W minimum was selected to ensure that the 150–200 nmi ADS-R separation could still support the dual-link ADS-B strategy as discussed in Sec. III.

The result in Figure 2 shows the reduction in operational capacity for scenarios (A) and (B) with 6-sector ground-based receive antenna at a 150–200 nmi spacing. The capacity estimate is based on receiving a message with 99.5% probability of success [9]. The total number of supported aircraft in this range is reduced from 350 aircraft in the unauthenticated case to 80 and 190 aircraft for scenarios (A) and (B), respectively. Also, for scenario (B), the authentication delay is at least nine seconds from broadcast of the original signed ADS-B message.

These estimates are somewhat pessimistic because recent advances in antenna design (e.g., a 12-sector ground receive antenna) and processing techniques can decrease interference. Still, the results are troubling. Given the predicted increase in air traffic—and the estimated 10,000 unmanned aerial vehicles operating throughout the national air space by 2030—this decrease in operational capacity may simply outweigh the benefits of digital signature broadcasts over the 1090 MHz channel.

One option would be to mitigate the interference with a multi-user modulation format that schedules transmissions in time, frequency, or code to limit interference [5]. A change of this magnitude to a nearly-operational protocol, however, is unlikely because of large signal definition inertia. Another option, which is potentially more practical and effective, would be to broadcast the authenticated messages in an alternate channel.

C. Alternative Authentication Channels

Instead of trying to retrofit digital signatures to the ADS-B protocol, would it be possible to transmit signed ADS-B messages over alternative channels? Imagine an alternative authentication channel over which signed ADS-B messages could be broadcast at the same rate as ADS-B messages at 1090 MHz or 978 MHz. Such an approach avoids the unpalatable reduction in operational capacity described in the previous section. The signed messages could take the structure suggested earlier, which consists of a 112-bit ADS-B message and its 448-bit ECDSA signature.

A variety of channels are worth considering to support signed ADS-B messages. Possibilities include the channels over which in-flight entertainment or internet connectivity are provided. Such high-bandwidth low-latency connections could transmit a signed ADS-B message to a ground network, which would then relay it to a central ATC database.

Another channel to consider is the protected Aeronautical Navigation Radio Service (ARNS) L-band at 960–1215 MHz where distance measuring equipment (DME) broadcast. The DME band consists of 252 1-MHz-wide channels where DME synchronization pulses and replies are transmitted. The transponder-based position-measurement DME system transmits in this 252 MHz of spectrum with exceptions for UAT transmissions at 978 MHz, Mode-S ES transmissions at 1030 and 1090 MHz, and Global Positioning System transmissions at 1176.45 MHz (L5 frequency).

Employing L-band for ADS-B authentication is enticing for several reasons. First, both Mode-S ES and UAT hardware already operate in the L-band, meaning that additional hardware and additional "holes in the airframe" to support more antennas are unnecessary. The result is a cost savings for commercial and general aviation. Second, the band is already ARNS-protected and allocated for aviation operations. Third, the frequencies allocated to UAT, Mode-S, and GPS L5 were actually re-purposed DME channels. This suggests that one or more 1-MHz-wide DME channels could similarly be allocated to support ADS-B authentication. Finally, the L-band is enticing because the FAA's alternative position navigation and timing (APNT) efforts has already considered this band to transmit additional data and navigation services with bit rates as high as 1000 bps [15].

A drawback of the L-band alternative is that the necessary spectrum redistribution would take significant, collaborative political and technical discussions involving major agencies, such as the FAA and FCC as well as international aviation agencies such as ICAO and EUROCONTROL. Furthermore, DME receivers would need to be replaced, unless they could be updated as part of a software upgrade. Still, if APNT and signed ADS-B message broadcasts could be packaged and implemented together, then only a single operational change could address two problems at once.

VII. Final Approach

NextGen's ADS-B air traffic surveillance protocol is unacceptably insure, but implementing a cryptographic enhancement would face significant regulatory and technical complexities. The most practical and effective cryptographic approach is one in which ADS-B broadcasts are signed with an asymmetric-key elliptic curve digital signature algorithm. Still, the burden of public-key management and the reduction in operational capacity over the 1090 MHz Mode-S ES channel would likely prove unacceptable to regulatory agencies, commercial airline companies, and general aviation enthusiasts. To avoid these difficulties, a possible alternative would be to broadcast signed ADS-B messages over a side channel such as the aviation-protected L-band at 960–1215 MHz. Meanwhile, ADS-B will continue to rely on radar for authentication—ironically, the very technology it was designed to replace.

References

[1] Special Committee 186, "Minimum aviation system performance standards for Automatic Dependent Surveillance Broadcast (ADS-B)," 2002, RTCA DO-242A.

[2] D. L. McCallie, "Exploring potential ADS-B vulnerabilities in the FAA's NextGen air transportation system," Master's thesis, Air Force Institute of Technology, 2011.

[3] A. Costin and A. Francillon, "Ghost in the Air(Traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Blackhat*, July 2012.

[4] D. Magazu, III, R. F. Mills, J. W. Butts, and D. J. Robinson, "Exploiting the Automatic Dependent Surveillance-Broadcast system via false target injection," *Journal of Aviation and Aerospace Perspectives*, vol. 2, no. 2, pp. 5–19, 2012.

[5] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *IEEE Aerospace Conference*, 2006.

[6] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 2040–2055, Nov. 2011.

[7] 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, TN, 2012.

[8] Federal Aviation Administration, "14 CFR Part 91: Automatic Dependent Surveillance–Broadcast (ADS–B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Final Rule," Federal Register, May 28, 2010.

[9] R. E. Boisvert and V. A. Orlando, "ADS-Mode S system overview," in *IEEE Digital Avionics Systems Conference*, Oct. 1993.

[10] K. D. Wesson, D. P. Shepard, and T. E. Humphreys, "Straight talk on anti-spoofing: Securing the future of PNT," *GPS World*, Jan. 2012.

[11] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *International Journal of Critical Infrastructure Protection*, 2013.

[12] W.-J. Pan, Z.-L. Feng, and Y. Wang, "ADS-B data authentication based on ECC and X.509 certificate," *Jounal of Electronic Science and Technology*, vol. 10, no. 1, pp. 51–55, Mar. 2012.

[13] R. V. Robinson, M. Li, S. A. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, and J.-U. Busser, "Impact of public key enabled applications on the operation and maintenance of commercial airplanes," in *AIAA Aviation Technology Integration and Operations Conference*, 2007.

[14] V. A. Orlando and W. H. Harman, "Project Report ATC-214: GPS–Squitter capacity analysis," in *MIT Lincoln Laboratory*, May 1994.

[15] S. C. Lo, B. Peterson, D. Akos, M. Narins, R. Loh, and P. Enge, "Alternative position navigation and timing (APNT) based on existing DME and UAT ground signals," in *Proceedings of the ION GNSS Meeting*, Portland, OR, 2011.