A Framework to Mitigate Airliner Risk in Air Traffic Management

Depeng Li
Department of Information and Computer Sciences
University of Hawaii at Manoa
Honolulu, HI, USA 96822
Email: depengli@hawaii.edu

Rui Zhang
Computer and Information Sciences Department
University of Delaware
Newark, DE, USA 19716
Email:ruizhang@udel.edu

***Abstract*—Threatened by hijacking or suicide-by-pilots, the airliner may either crash itself or be shot down due to its potential for suicide attack. To save persons on board, some researches allow air traffic controllers or federal agents to take over authority for airliner piloting. Though rarely, an air traffic controller may possibly misuse this privilege and then attack airliners, too. In this paper, to mitigate such risks , we propose a framework which is composed of a few critical components based on existing cryptographic schemes. Experiments are designed to simulate the real world cases and results demonstrate that our solution is efficient and feasible for current air traffic management.**

I. Introduction

Safety concerns are worthy of been paid close attentions to in aviation establishments due to the fact that a considerable number of human lives are always at stake. According to the International Civil Aviation Organization (ICAO), some 3.2 billion passengers have utilized the commercial airliner in 2014 and the annualized passenger figure is expected to be 6.4 billion by 2030 [21]. However, flying involves risks: as one of the most terrifying risks, hijacking or suicide-by-pilot [16], may not only kill the persons on board but also result in suicide attacks i.e. massacring people on the ground. As an example, in the September 11 attack, 265 persons aboard airliners were killed and the suicide attack also claimed 2731 lives on the ground.

The hijacking or suicide-by-pilot is partially resulted from the access control vulnerability, e.g. . The flight control system follows the interleaving between the Pilot-In-Charge (PIC, interchangable with pilot, hereafter) and auto-fly pilot (auto-pilot, in short) [37]. The pilot is the final authority for the safety operation of the commercial airliner. PICs supervise the auto-pilot system and can override the auto-pilot when necessary. Meanwhile, PICs should comply with the air traffic controller (ATC) who oversees the area. In an emergency that requires immediate actions, PICs can deviate from ATCs' instructions to the extent which is required to meet the emergency [20]. Nevertheless, being the most creative and valuable element in modern aviation systems, pilots could also be a vulnerable part: around 75 percent of all accidents result from improper human factor related behaviors [1], which include hijacking and suicide-by-pilots occurring 369 and 19 times since 1985, respectively [16].

Since pilots are the ultimate authority, pilot errors in current flight control systems are critical: *(1)* pilots may be manipulated by hijackers on board: on September 11, 2001, terrorists hijacked four air-planes and carried out suicide attacks [38], *(2)* pilots may deliberately crash an airliner: in 2015, Andreas Lubitz, the co-pilot, overrode auto-pilots' privilege and flew Germanwings Flight 4U 9525 into a mountain committing murder-suicide [17], and *(3)* pilots can operate the airliner contrary to ATCs' instruction but ATCs cannot enforce their legal will on pilots: ignoring instructions from ATCs, Gamil el-Batouty, the co-pilot of an Egypt Air flight 990 deliberately crashed the airplane into the Atlantic Ocean resulting in 217 deaths in 1999 [19].

So far, there are a few means to handle hijacked airplanes. (1) The most frequently used counteraction is to shoot down the aircraft to avoid suicide attacks: 109 hijacked aircraft have been shot down in the last three decades [16]. In September 11, Vice President Cheney issued an order to shoot down hijacked aircraft [27]. (2) Furthermore, to mitigate pilot-related risks, some safer countermeasures are proposed to replace the deadly force - the shooting down. Boeing and Honeywell proposed a patent, the Boeing Honeywell Uninterruptible Autopilot (BHUAP) to take over pilots' authority by ATC or federal agents in emergencies of hijacking [35]. In BHUAP, ground ATCs or federal agents can activate the automatic flight mode via forwarding control instructions through the digital radio communication channel (e.g. Automatic Dependent Surveillance-Broadcast (ADS-B) [29], [11]). The channel links the ground air traffic control stations and the e-enabled airplane [9], [40]. Once the mode is activated, nobody aboard can turn it off and the airliner will be landed automatically at a nearby airport. It benefits from advanced technologies in aviation: in recent years, the air traffic management (ATM) is facilitated by the integration of aviation communication technologies [11] and [29], e-enabled airplane [26], and remote control technologies.

However, there are a few pressing challenges in BHUAP. The airlines and pilots union cannot adapt BHUAP without carefully addressing challenges such as potential attacks for the digital communication channels, misusing of access control privileges, etc. [18]:

- To reduce the risk of single point of compromise for pilots, ATCs are granted the privilege to take over the

control right of the airplanes. But ATCs may also be vulnerable of the single point of compromise. Thus an appropriate access control mechanism is highly demanded to prohibit one single compromised ATC from misusing the taking-over privilege;

- Without the security mechanism, the terrorists/hacker may manipulate the digital communication channel which is used to forward control instructions from the ground ATC to the e-enabled airplane. Therefore, injected and/or altered control instructions could be issued by the hacker to highly impact the airliner safety;

- The high packet loss/error rate over ADS-B communication channel in dense air space has already been observed [29]. When delivering the safety-critical instructions in this condition, our solution should be fault-tolerant to avoid the unreliable data communication with zero packet loss.

In this paper, in order to mitigate the security risk resulted from BHUAP system, we present a new framework. As the best of our knowledge, we are the first to address the challenges early mentioned. The proposed framework is composed of the following three components by leveraging some existing schemes:

- *Threshold Access Control Mechanism*: When an ATC takes over PICs' authority, it is possible that (a) the ATC is compromised or (b) the ATC's credential is stolen. To conquer the single point of compromise, we construct a couple of threshold access control mechanisms that can prevent one single malicious / compromised ATC from manipulating the pilots' privilege, one is *efficient-oriented* by using XOR-operation secret sharing scheme [32] and the other is *attribute-oriented* by using attributed-based encryption (ABE) algorithm [6]. The former prioritizes computational cost and the latter concentrates on combinations of varied attributes.

- *Trust-based, Unequal Secret Sharing and Trust-based Delegation ABE*: In a (t, n) threshold access control method, to deal with scenarios that there are less than t ATCs online, we propose *(1)* the trust-based, unequal secret sharing based on XOR-operation secret sharing and *(2)* the trust-based delegation for ABE. ATCs' trust values are calculated by existing trust evaluation system.

- *Reliable and Authenticated Protocol (RAP)*: It is necessary to provide fault tolerant solutions due to the high rate of packet loss and high possibility of message collisions over ADS-B communication channel in dense space. Since the aviation system cannot afford any packet loss when transmitting the safety-critical instruction, we present the reliable digital communication based on the information dispersal algorithm (IDA) [24], [23]. We also provide authentication service over ADS-B digital communication based on the BLS short signature scheme [8] since its short length aligns with ADS-B's short frame of data-block (e.g. 56/112 bits long).

II. Background and Related Works

A. Background

1) Air Traffic Management: With the continuous growth of air traffic demand as well as requirements for more secure and reliable data communication, the paradigm shift from traditional ATM to advanced ATM system is necessary. In detail, the ground-based navigation system is replaced with satellite-based communication system, the verbal communication and ground radar system is switched to more accurate and more reliable digital communication (e.g. ADS-B) and the e-enabled aircraft is substituted for traditional ones. Therefore, the modern, underway ATM system could accommodate much more aviation applications such as safe decision making system [13], conflict detection and resolution, and 4-D trajectory based operations [26]. In a word, the current ATM system properly incorporates the sophisticated sensing and monitoring technologies enabled by more reliable digital communications with real-time situational awareness for both pilots and air traffic controllers [13] and [42].

2) Wireless communication for aviation: Boeing Communication and ADS-B: Boeing: To enable remote access of ATCs for an airliner via cyber communication channel, Boeing airplanes leverages the existing data communication methods and data link network routing technologies: remote ATCs could communicate with aircraft via radio or satellite communication channels [12], [36]. The Aircraft Communication Addressing and Reporting System (ACARS) can transmit data between the Flight Management System (FMS) of airliners and ground stations (airports, aircraft maintenance bases, air traffic control, and so on) via radio and satellite technologies [25]. The aircraft data link network routing technology [31] could provide packet routing function [3]. To ensure security, BHUAP invokes an aircraft specific encryption key in ATC/military or other aviation carriers [9]. Thus, the *e-enabled airliner* [26] could be connected with a global information network [33] with the protection of security services.

ADS-B: ADS-B is developed to replace traditional radar-based system: ADS-B broadcasts the plaintext messages over radio transmission links within almost each second. In detail, at the physical medium level, ADS-B operates the active interrogation from ATC towers or radars at the 1030 MHz radio frequency and from aircraft at the 978/1090 MHz. At the data-link level, ADS-B performs with a data rate of 1 Mbit/sec, messages are encoded with the block size as 56 bits or 112 bits [11]. However, so far, even as the advanced data communication technology, ADS-B demonstrates the weak reliability: ADS-B experiences packet error rates above 50 percents due to the severe message collisions in dense air space [29]. Furthermore, basic security services such as authentication have not been fully provided [29].

3) E-Enabled air traffic control: Air traffic control systems are developed to transmit critical information between ground ATCs and e-enabled airliners [26]. Airliners periodically broadcast [10] identities, accurate states (e.g. position,

altitude, speed, etc.), and other messages (e.g. waypoint) to ground ATCs [22]. ATCs can issue tasks and other airplanes' situation awareness information to pilots [5] and [41]. These messages could be used by ATC to analyze the airline's states and could also be shared with other airliners [4].

4) BHUAP system to activate taking-over button: BHUAP [9], [40] is designed to prevent hijacking. Generally, in an aircraft, a crash-warning device is connected with cockpit computers. When hijackers force the pilots to crash the airliner or pilots themselves deliberately to do so, audible warnings from crash-avoidance systems are triggered. If PICs keep on ignoring this alarm, ATCs could trigger the BHUAP mode remotely. It is difficult to turning off BHUAP: Relayed by the Flight Control Computer (FCM), BHUAP connects with a separate, independent power supply. This prevents the compromised pilots or hijackers from turning off the crash warning system or BHUAP [30].

B. Related Works

The following schemes have been utilized in the general distributed networks. However, they have not been deployed in either aviation systems or air traffic control systems because (a) both systems have their uniqueness which prohibits the direct utilization of those schemes and (b) considerable works such as customization and verification for those schemes are required. In this paper, we endeavor to bridge the gaps and realize our security goals. They are introduced below: *(1) Threshold-based Access Control*: Shamir's *(t,n)* threshold-based secret sharing [28] is utilized as primitives for cryptographic applications. *(2) Attribute-Based Encryption (ABE)*: Ciphertext-policy Attribute-Based Encryption (CP-ABE) scheme [6] has been developed so the fine-grained access control could be achieved. *(3) Trust systems*: the trust system includes a Trust Computation Engine [2] which is used to calculate trust values.

To guarantee a reliable multicast service for authentication information, Park, Chong and Siegel [23] proposed the Signature Amortization Information Dispersal Algorithm (SAIDA) to encode authentication information with Rabin's Information Dispersal Algorithm (IDA) [24].

III. Problem Formulation and Threat Model

In this paper, the air traffic control system consists of (i) an e-enabled airliner, (ii) two kinds of users, one is the pilot and the other the ATC, (iii) a number of air traffic control computers (they are used by ATCs, located in air traffic control stations and connected with each other via LAN/WAN), and (iv) key servers which manage secret shares, secret values, and keys, (v) control server which is located in the air traffic control station and its function is to forward control instruction toward e-enabled airliners, and (vi) ADS-B wireless digital communication link connecting both control servers and airliners.

An ATC is denoted by $A_j \in A = \{A_1, A_2, ..., A_n\}$ *where* $1 \leq j \leq n$ and A is a set of ATCs. Each ATC A_j is associated with a credential Cr_j. By using Cr_j, an ATC A_j could be granted the access right to the ATC computer located in air traffic control stations. A pilot is defined as P_i. As the final authority on board, P_i controls the dashboard within the airliner. We assume that the airline has already deployed a BHUAP device which is embedded within pre-programmed firmware. Its function is to disable/override pilots, P_i's operating authority on board. Meanwhile, as a general deployment, a ground proximity warning system (GPWS) [34] is installed on the airliner so that the alarm could be triggered once the crashing risk is detected. Working in the air traffic control station, A_j may notice that the pilot, P_i's malicious operations or the GPWS is triggered to ring the alarms but the pilot P_i keeps ignoring the audible warnings. At that time, the ATC A_j could execute his/her privilege to make a decision: the instruction to take over a pilot A_i's authority is forwarded from the control server (CS) to the airliner's BHUAP through ADS-B channels.

A. Problem Formulation

Malicious or poor-performance ATCs could threaten airliner safety through misusing access rights to withdraw pilots' authority. If any ATC could activate the BHUAP button to withdraw pilots' authority, the airliner safety is under the risk of the single point of compromise. The reason lays in the fact that any ATC could act maliciously. Here are a few scenarios: **(1)** A malicious ATC A_j Charlie could withdraw pilots P_i's authority whenever A_j login and accesses an ATC computer by inputting his user account and credential Cr_j. **(2)** A honest ATC A_x Alice has her own credential Cr_x which has been stolen by A_j Charlie. A_j Charlie could commit malicious decisions via using ATC A_x's credential Cr_x. **(3)** Assume that some air traffic control systems require that only ATCs with high ranks e.g. at the manager level have the privilege to take over pilots' authority. However, attacks in either (1) or (2) could also happen for ATCs with a high rank. **(4)** Assume that we proposed an access control mechanism in which at least t ATCs' approvals are required. Also assume that there are more than t ATCs working in the same site/station. If occupying the site, a group of terrorists can force t ATCs taking over pilot P_i's authority together. This, namely, "single site of compromise", also threatens the safety of the airline. Thus, an appropriate access control mechanism is highly demanded so that an ATC A_j's privilege to take over pilot P_i's authority could be fairly limited.

B. Threat Model

The threat is that both pilots and ATCs could act maliciously. In our threat model, we assume that it is possible that the compromised pilot/ATC could be allowed to operate the airliner/ATC PC in an extreme dangerous way due to a number of potential causes including psychological problems (e.g. suicide), health problems (e.g. heart attack), and being threatened by other persons (e.g. terrorists, gangster). The malicious pilot P_{bad} can mislead, fool, or attack his/her colleague in the cockpit. Thus, the malicious pilot P_{bad} can fail "two-person" policy and commit suicide-by-pilots or even the suicide attack against targets on the ground or in the sky or others. The malicious ATC could misuse the taking over privilege on ATC PC to activate BHUAP function. However, we assume it is hard for the pilot or ATC to successfully break modern cryptographic primitives such as digital signing, threshold

secret sharing and ABE encryption. We also assume that devices within the airliners or PC in ATC station are tamper-resistant so that the pilots/ATCs cannot either compromise them or extract cryptographic keys stored in them.

C. Goals, Scope, Assumptions, and Limits

Goals: the proposed solutions should satisfy the following security requirements **(a)** overcoming the single point of compromise, **(b)** supply of efficiencies, **(c)** support of the "different sites" policy, **(d)** handling the lack of t ATCs online in threshold access control mechanism, and **(e)** dealing with both packet loss and unauthenticated protection in ADS-B. This paper attempt to propose a set of solutions which could prohibit malicious pilots/ATCs, P_i/A_j or hijackers/hackers in an efficient, reliable, secure and authenticated way. To achieve this goal, the proposed countermeasure should satisfy the following security requirements *(i) threshold access control for BHUAP*: provide a threshold access control mechanism to limit the privilege of one single ATC. *(ii) resilience for lack of t ATCs*: present flexible solution while lack of ATCs, *(iii) efficiencies*, due to the real-time requirement and the increase of traffic demands, the proposed solution should be executed in an efficient way, and *(iv) reliable and authenticated communication*: the quality and authentication service for ADS-B should be enhanced.

Scope and Future Works: This paper only focuses on limiting ATCs A_j's privilege of overriding pilots' authority. Other issues are out of scope: Why ATCs/pilots could be compromised are out of the scope of our paper. Furthermore, how to promptly detect the hijacking or the suicide-by-pilot is important for the airliner safety but they are also out of the scope and will serve as our future research. Moreover, this paper will not counteract other attacks that could damage the airliner ranging from destroying the circuit breakers in the cockpit to disconnecting electrical systems causing a fire or malfunction. In addition, ADS-B communication channel may be targeted by hackers who launch attacks such as Denial of Service (DoS) attacks, radio interference attacks, etc. How to counteract them is out of our scope. Last but not the least, since the (t, n) threshold-based secret sharing is adapted to fit in our solution, how to determine the concrete value for both t and n is critical but they cannot be decided until a practical field test of the implementation of our solution in a real aviation system. It has to be put in our research plan in future.

Assumption: Like other research in the security areas, we assume that the majority of ATCs (particularly, t out of n, OR at emergent case t' out of n where $t' < t$) are honest and trustful. Meanwhile, we assume that devices in the aircraft such as FCM, BHUAP, GPWS, etc. are tamper-resistant. Device attestations are assumed to be deployed to validate device on board. Furthermore, we also assume the availability of public key infrastructure (PKI) in the aviation system. In addition, we assume that the communication channel between ATC station and e-enabled airliners exists.

Limits: This paper can only mitigate but not eliminate risks introduced by malicious ATCs. There are other existing risks e.g. wireless communication interference but they cannot be comprehensively studied and addressed in this paper.

IV. Proposed Access Control Solution

In this section, we first describe the system model that includes both the system architecture and four layers. Second, we will explain how to accomplish the trust-based, unequal, XOR-operation secret sharing scheme and trust-based delegation ABE in subsection IV(B) and subsection IV(C), respectively. Third, the reliable and authenticated protocol (RAP) over ADS-B between the control server and the e-airplane will be explained in subsection IV(D).

A. System Architecture of Proposed Solutions

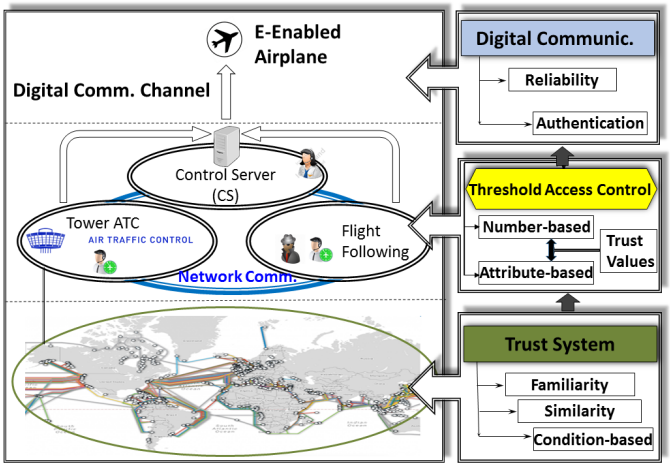

Fig. 1: System Model of Proposed Solution

As depicted in Figure 1, the proposed system architecture consists of four layers which are explained below:

(1) Trust system layer: We deploy some existing trust calculation engine to assess each ATC's trust value which could be used by the threshold access control mechanism in the air traffic control layer.

(2) Threshold-based access control in air traffic control layer: one single ATC can decide on whether a pilot's authority should be overridden or not. To counteract the single point of compromise for one single malicious ATC, we deploy both a XOR-operation threshold access control [32] and the attribute-based encryption (ABE) [6] to achieve the t, n threshold access control goal. Both the secret share distribution and the secret share reconstruction are provided. However, the secret share, sometimes, cannot be reconstructed due to the lack of t ATCs online. We further address the challenge via trust-based, unequal, secret sharing scheme and trust-based delegation ABE.

(3) Digital Communication and Control Server layer: In this layer, the control instruction is protected and delivered by our RAP protocol from the control server to the e-airplane via digital communication channels (e.g. ADS-B [29]). Our RAP protocol presents reliability and authentication services based on IDA algorithms [24] and BLS short signing scheme, respectively.

(4) E-enabled airplane (e-airplane) layer: in this layer, the e-airplane could receive and verify the digitally signed instruc-

tions sent from the control server. If verifying, it activates the BHUAP mode.

B. Trust-based, unequal, XOR-operation secret sharing

In this subsection, we focus on designing an efficient (t, n) threshold access control scheme to handle two scenarios, one with less than t but larger than t' ATCs online and the other with at least t ATCs. It could satisfy the following requirements: (1) *single point of compromise resilience* (2) *efficient computation*, and (3) *secret reconstruction with less than t ATCs online*. When there are at least t ATCs online, [32] already proposed the most efficient secret sharing scheme relying on XOR-operations. Based on [32], we make our contribution to handle the scenario with less than t ATCs online. Since only XOR-operations on binary strings, cyclic shift operations, addition, and floor of number operations are required, our solution, like [32], are efficient.

Note that our (t, n) threshold secret sharing scheme are designed over general finite field $F = GF(q)$. However, our solution lets $q = 2$. Thus, all operations are processed over sequences of binary numbers and that is the reason why our solution is efficient.

Then, we introduce our assumptions: (1) assume that S is the secret value (i.e. a sequence of binary numbers) which is defined as $S = S_0 \cdots S_{\tau-1} \in F^{\tau} where \tau = |S| \geq n$. (2) let p be a prime number with $gcd(p, q) = 1$ and $p \geq \tau + 1$. (3) let the symbol $< a >_p$ denote an integer b *where* $b \in \{0, \cdots, p-1\}$, a is an integer, and $b \equiv a(mod p)$. (4) let t_{min} be the minimum number of ATCs online. Since the air traffic control system is regulated by different organizations, t_{min} could be varied in different countries. But, for a particular country, the code of corresponding governments should or will predefine it to guarantee the aviation safety. (5) let $T(A_j)$ denote the trust value of an ATC, A_j. $T(A_j)$ is calculated by our trust system which is described in section 4.4.

Outline of our secret sharing scheme: Our secret sharing scheme is defined as $SR(t, n, p-1)$ over $F = GF(q)$. They are treated as a set of $(p-1) \times (p)$ matrices, each of which is named as $\mathbf{M}$. Thus we can say that $SR(t, n, p-1)$ is composed of all $(p-1) \times (p)$ matrices. Each of matrix, $\mathbf{M}$, consists of $(p-1) * p$ elements, namely, $c_{i,j}$. Then, we define a matrix $\mathbf{M}$ in formula (1):

$$\mathbf{M} = \begin{cases} c_{i,0} = s_i, & \text{if } 0 \leq i \leq \tau - 1 \\ c_{i,0} = 0, & \text{if } \tau - 1 < i \leq p - 1 \\ c_{i,j} = \sum_{j=0}^{n} c_{<m-jl>_p}, j = 0, & \text{if } 0 \leq m \leq p-1 \\ & \text{and } 0 \leq l \leq n-t-1 \end{cases} \tag{1}$$

Like other secret sharing secret, our secret sharing scheme is composed of the *secret distribution* and the *secret reconstruction* phases, both of which are described below:

Secret Distribution and Reconstruction: we will use a matrix $\mathbf{M} \in SR(t, n, p-1)$ as our distributed secret. Briefly, the i^{th} column vector of matrix $\mathbf{M}$ will be released to the i^{th} participating ATCs where $0 \leq i \leq t$. We then explain steps in detail below:

Let us describe how to convert a $[n, t, d]$ maximum distance separable (MDS) code into an optimal information rate and linear (n, t) threshold sharing scheme where $d = n - t + 1$. We further assume that $GF(q^m)$ is a finite field and let $g(z)$ be the generator polynomial over $F = GF(q^m)$ for the Reed-Solomon code.

$$\begin{aligned} g(z) &= (z-1)(z-\alpha)\cdots(z-\alpha^{n-k-1}) \\ &= g_0 + g_1 z + \cdots + g_{n-k} z^{n-k} \end{aligned} \tag{2}$$

Let us define the other polynomial with degree $t-1$ for information symbols $(f_0, f_1, \cdots, f_{t-1}) \in GF(q^m)^t$: $f(z) = f_0 + f_1 z + \cdots + f_{t-1} z^{t-1}$. Then, we multiply $g(z)$ by $f(z)$ and its result $m(z)$ will be used to encode the secret sharing value S.

$$\begin{aligned} m(z) =& g(z)f(z) \\ =& g_0 f_0 + (g_0 f_1 + g_1 f_0) z + \\ & (g_0 f_2 + g_1 f_1 + g_2 f_0) z^2 + \cdots \end{aligned} \tag{3}$$

Based on formula (3), let us construct an new a row vector $(c_0, \cdots, c_{n-1})$. Let the secret share value $s = c_0 = g_0 f_0$. The rest $n-1$ coefficients, namely $c_1, c_2, \cdots, c_{n-1}$ are distributed to $n-1$ participating ATCs one to one through predefined secure channels, respectively. Then, let $c_n = f_0 + \cdots + f_{t-1}$. All this makes it a (n, t) secret sharing scheme. Figure 2 illuminates the details.

Let us construct a polynomial over $F = GF(p)$ with its degree $d \leq p-1$, the purpose of which is to calculate the secret shares that will be distributed to each ATCs later. Let $M_p(x) = \sum_{i=0}^{(p-1)} x^i$ denote the polynomial and let R_p be the rings of $M_p(x)$. We also assume there is a root, α for $M_p(x)$

$$(c_0, \quad c_1, \cdots, c_{n-1}) = (f_0, \quad f_1, \cdots, f_{k-1}) \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & g_{n-2k+1} & g_{n-2k+2} & \vdots & g_{n-k} \end{pmatrix}$$

Fig. 2: Coding Process of XOR-based Secret Sharing Scheme

in ring R_p which satisfy $\alpha^p = 1$. Based on the denotation above, we define $r \times p$ matrix $\mathbf{H}$ where $r = p - t < p$

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(p-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(r-1)(p-1)} \end{pmatrix} \quad (4)$$

Let C be a linear code of length p over ring R_p with $\mathbf{H}$ as the partial matrix. We can observe that the determinant of each $r \times r$ sub-matrix of $\mathbf{H}$ has multiplicative inverse in R_p which results in the rank r of $\mathbf{H}$. We further deduce that the secret sharing scheme $SR(t, n, p-1)$ over $F = GF(q)$ is equivalent to C_s where

$$\begin{aligned} C_s = \{(c_0, c_1, \cdots, c_{p-1}) \in C : \\ c_0 =< s_0, \cdots, s_{\tau-1}, 0, \cdots, 0 >\} \end{aligned} \quad (5)$$

We then define the generator polynomial for C over ring R_p as $g(z) = g_0 + g_1 z + \cdots + g_r z^r$. Thus, considering that g_0 is multiplicative inverse in ring R_p, there must exist $f_0^s \in R_p$ such that

$$f_0^s \cdot g_0 =< s_0, \cdots, s_{\tau-1}, 0, \cdots, 0 > \quad (6)$$

Therefore, for any polynomial $f(z) = f_0^s + f_1 z + \cdots, + f_{t-1} z^{t-1}$ with random $f_1, \cdots, f_{t-1} \in R_p$, $f(z)g(z)$ could work as the secret share distribution. Our idea is that we distribute not one secret share but more i.e. α_j column vectors to participating ATC, A_j. Assume that a set of ATCs $\{A_1, \cdots, A_{t_{min}}\}$ work as a group to reconstruct the secret value. For each ATC A_j, in formula (6), we calculate the number of secret shares they should be distributed. Here, assume ATC A_j could be issued α_j secret shares. The weight α_j will be calculated based on ATC A_j's trust value, $T(A_j)$ and other ATCs. (Refer to subsection IV(D) for details regarding trust value evaluation).

$$\alpha_j = \left\lfloor \frac{T(A_j)}{\sum_{j=0}^{t_{min}} T(A_j)} t_{min} + \frac{t}{t_{min}} \right\rfloor \quad (7)$$

Thereafter, the equation (3) together with matrix generated in figure 2 could be solved to generate the secret shares or the symbol $< f_0^s, f_1, \cdots, f_{k-1} >$ (and randoms $f_1, \cdots, f_{t-1}$) together with polynomial $g(z)$ could be utilized to generate the secret shares. Each ATC A_j will be randomly distributed α_j secret shares. Therefore, we could collect t secret shares from t_{min} ATCs and based on the decoding procedure in [7], we can reconstruct the secret value, $g_0 \cdot f_0$ as replacing z with 0. If we accomplish the secret sharing scheme on the finite field as $F = GF(2)$, the computational cost is $O(r(p^2 + r))$ [7] and the operations are solely XOR operations.

C. Reliable and Authenticated P-2-P Communication Link

Due to the existence of severe packet loss (i.e. the ADS-B experiences around 50 percent packer error rate resulted from message collisions in dense air space) as well as the lack of authentication service [29], we propose a reliable and authenticated communication protocol over ADS-B from control server to airliners.

Selection of Authentication Scheme: The authentication scheme to authorize the point to point communication between the air traffic control stations and the e-enabled airplane should satisfy three requirements, (1) efficient computational cost, (2) less communication overhead, and (3) simple key management. The BLS short signature scheme is selected after comprehensive comparison with other solutions such as (1) HMAC plus symmetric key encryption schemes, (2) One-Time Signature (OTS) schemes, and (3) other public-key systems (RSA digital signatures).

Reliable Communication Algorithm: we propose an (n, m) reliable algorithm based on the reliable communication scheme, Modified Signature Amortization Information Dispersal Algorithm (M-SAIDA) where m is the number of bits and n is the number of forwarded bits with $m < n$ in communication channel [14]. This is a modification of SAIDA proposed in [23]. Our algorithm satisfies the requirements of zero packet loss and computational efficiency. For detailed algorithm, refer to our previous work [14].

Reliable and Authenticated Protocol (RAP) Our RAP protocol is designed to take over pilots' authority. In details, *(1)*, the control server (CS) generates the signature S by signing both the instruction (I) and the timestamp (TS) via using BLS short signature algorithm [8] with CS's private key $PRI - K_{CS}$. Next a message composed of the signature S, the instruction i and the timestamp TS are encoded by algorithm 1 *IDA-Encode* and then forwarded to airliner (AL). *(2)*, after receiving the message, the airliner (AL) invokes algorithm 2 *IDA-Decode* to get the message, i.e. S, I, and T. After that, S is verified by BLS verification scheme with CS's public key $PUB - K_{CS}$. (3) After executing instruction I, the airline (AL) should feedback the CS its subsequent states. The message should be authenticated by its own private key $PRI - K_{AL}$ and it freshness should be presented with the timestamp (TS). But we will not provide details for this step since it is general. Note that the instruction I encapsulated in each step should contain the corresponding airliner's ID, ID_{AL}. Steps are listed below:
1: CS $\rightarrow$ AL: S = IDA-Encode($I||T||SIGN_{PRI-K_{CS}}\{I||T\}$)
2: AL $\rightarrow$ CS: IDA-Decode($VERIFY_{PUB-K_{CS}}(S, I||T)$)

V. Experiments and Analyses

A. Performance Evaluation

In this subsection, we will evaluate the performance of the proposed solution. In detail, we will carefully evaluate four fundamental components: (1) the trust-based, unequal, secret sharing scheme which mainly relies on XOR operations and a few division operations. (2) Trust system does not emphasize on performance, (3) ABE scheme, (4) IDA schemes which process matrix multiplications, and (5) RAP protocol which invokes BLS short signature signing and verification operations. The details are analyzed below:

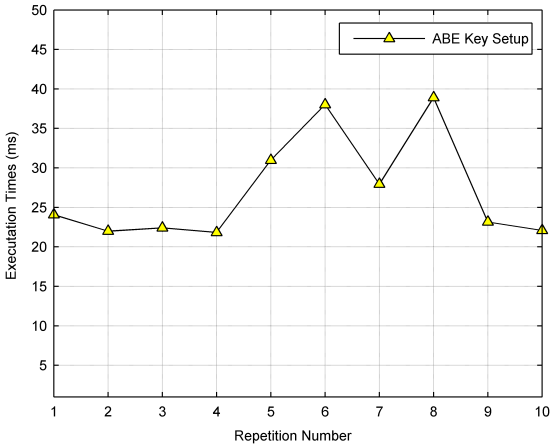

Fig. 3: ABE Key Setup

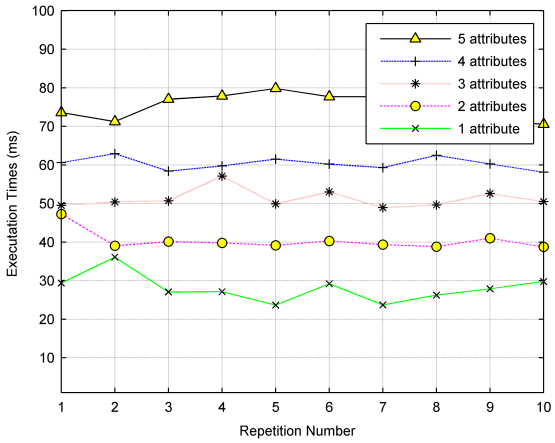

Fig. 4: ABE Key Generation

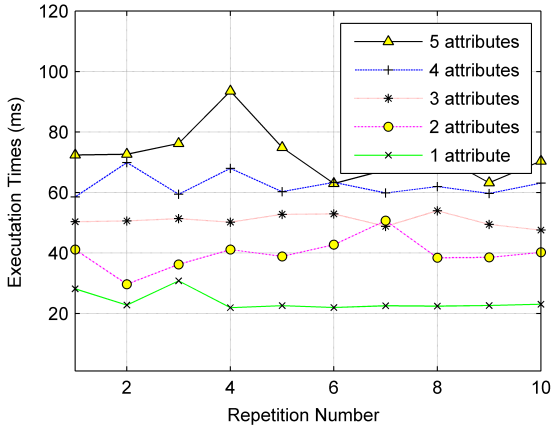

Fig. 5: ABE Encryption on PC

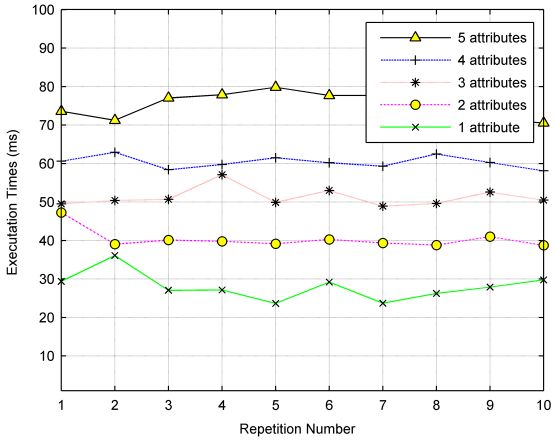

Fig. 6: ABE Decryption on Key Server

XOR-operation secret sharing scheme: As we analyzed in subsection IV(B), if we let $q = 2$, our operations are executed over binary sequence. Thus, only the XOR operations are executed which is efficient. If we accomplish the secret sharing scheme on the finite field as $F = GF(2)$, the computational cost is $O(r(p^2 + r))$ [7] and the operations are solely XOR operations. Meanwhile, our trust-based, unequal, secret sharing scheme need calculate the number of secret shares which should be assigned to each ATC. During the process, $t_m in+1$ times' addition, two times divisions, and one multiplication are required for each ATC. Thus, the computational cost is trivial and that is why we do not to evaluate its execution time in subsection V(C).

Trust system and delegation of ABE: the trust system is mainly accomplished via survey, report and data input. To calculate the trust values based on the data captured above is not so important. Furthermore, the trust calculation engine based on formula (8) is mainly composed of number multiplication and number addition. The performance cost is trivial and we do not measure it further. The delegation of ABE is discussed in preious research *attribute-oriented*.

IDA encoding and decoding scheme: The performance of our IDA algorithms in RAP protocol will be analyzed in terms of both communication overhead and computational cost. Assume that the message size is m and the message size generated by IDA-encode is n where $n \leq m$. Then, the communication overhead is n and the redundancy rate is (n/m). The computational cost for the IDA-Encode algorithm is n and that of the IDS-Decode is $O(m)$. In terms of the actual packet loss, it normally follows the burst rather than

TABLE I: Execution times: BLS signing and BLS verification (repeated eight times)

Operations	**BLS signing operation**								—	**BLS verification operation**						
Execu.times (ms)	0.08	0.05	0.03	0.07	0.01	0.23	0.21	0.12	2.75	2.21	2.33	2.1	2.21	2.6	2.2	2.31

the independent model. In [39], the 2-state Markov chain (2-MC) loss model is introduced. In [15], the Biased Coin Toss (BCT) loss model is introduced. Both of them can accurately model bursty loss patterns. [23] analyzes the authentication probability, $Pr\{P_i verifiable | P_i is received\}$ of IDA using the two loss models. The result suggests that making the block size large could decrease the communication overhead if relatively long verification delays are tolerated. However, this does no align to our ATM system. Therefore, future research should be focused on this topic to study the aviation communication and ADS-B's packet loss model.

RAP protocol: In our RAP protocol, the reliability service is provided by IDA encoding and decoding. The authentication service is supported by BLS short signing scheme: the first step executes one BLS signing which includes one hash function operation and one elliptic curve exponentiation operation; the second step executes the BLS verification which invokes one hash function operation and two bilinear pairing operations over curves. The experiments results are demonstrated at Table I and the detailed configuration is referred to subsection V(C).

B. Security Discussion

In this subsection, we discuss the security issue introduced by the threshold secret sharing, ABE scheme as well as the PAR protocol. As the trust calculation is not so closely related with the security issue, we will not analyzed it here.

Trust-based, unequal, secret sharing: in this scheme, we assume that the secre share distribution and the secret share collection are undertaken in secret channel. Therefore, there should be secret information leakage in this phases. Actually, as one of the most restricted network, the ATM system mainly utilizes LAN/WAN to connect each air traffic control station together. The secure communication technologies utilized in the security-related organization is mature and we could trust the security protection upon such kind of network communication settings. Accoording to the code of aviation system, the t_{min} ATCs should be online at any time slot, the number of ATCs could be guarantee. Since they, $\{A_1, A_2, \cdots, A_{t_{min}}\}$ are distributed t secret shares altogether and there are no duplicate between each other, we can deduce that at the decision making, all t secret share could be collected if they all agree to take over the pilot's privilege. Therefore, the secret value s could be reconstructed. Thus, the security of trust-based, unequal secret sharing scheme can be presented.

Trust-based Delegation ABE: The security of ABE including its delegation primitive is already proved in [6]. Our trust-based delegation is to add one new gater associated with the comparison of two trust values. Since the whole random values e.g. r, $\forall j, \tilde{r_j}$ are renewed. Thus our new delegation's security, like ABE, could be provided.

RAP protocol: In this protocol, the BLS short signature signing and verification technologies are provided. Therefore, the authentication service could provided. Since its public/private key management is a well-known, general solution, we do not explain it in this paper due to space limit. Thus, we can assume that the normal key management issues such as key revocation, key refreshment, key distribution, etc. could be presented. During the digital communication over ADS-B channels, since the timestamp is encapsulated in each packet, the man-in-the-middle attacks could be prohibited. In PAR, we also deigned that the messages should include the destitution ID and source ID in a good sequence, the oracle attack could be prevented. Therefore, PAR protocol is secure.

C. Experiments and Results

We implement the ABE components based on Pairing-Based Cryptography (PBC) library [29] built on the GNU Multiple Precision arithmetic (GMP) library [1]. GMP library provides arbitrary precision arithmetic APIs which are invoked by PBC to support pairing-based cryptosystem. In our application, we use the pairing-friendly elliptic curves $E(F_{(2^{379})}) : y^2+y = x^3+x+1$ and $E(F_p) : y^2 = x^3+Ax+B$ with a 512-bit prime. Furthermore, to satisfy the performance requirement, we deploy MNT elliptic curve to implement the ABE system. MNT elliptic curve of embedding degree 6 with order 160 bits length and base field order 512 bits length were utilized. We collected ten times' (randomly selected number) executions of ABE operations, the average of which are depicted at Fig. 3 - Fig. 6, including ABE Setup, ABE key generation, ABE Encryption, and ABE Decryption respectively. The control server and the ATC PC in the experiment were both virtual machines hosted by Oracle's VirtualBox installing Ubuntu 11.10. The detailed configuration of Control Server / ATC PC is Memory-4GB; CPU-2.67GHz; Disk-7.9GB. We customize the Ubuntu Operating System in VirtualBox in such a way that only the command line components (e.g., text editors, g++ and gcc, socket functionality and SSH client and server) are deployed and other packages (audio player, media players, and other GUI applications) are removed. Then, the experimental result shows the much more close to practical results. In Fig. 3-6, we illuminate the schemes' performance when executing them on our platform. The average values of experiment results (the execution is repeated 10 times) above are demonstrated, in which, the ABE encryption at a ATC PC and the ABE decryption at a control server executes less than 170ms and 260ms respectively when the number of attributes is 5 or less. The ABE communication overhead is high but still affordable.

BLS short signature signing and BLS signature verification are executed on virtual machines mentioned early. Each of them are executed 8 times. In Table I , we list the results which show that the execution times of BLS signing and verification are less than 0.23 ms and 2.75 ms, respectively. We conclude that they are feasible in the ATM system.

The performance of our trust-based, unequal secret sharing scheme are analyzed in subsection V(C). Since they are solely based on XOR operations which demand significantly trival execution times, we will not operate any experiments for them since the performance is predictable.

VI. Conclusion

Airliner incidents indicate that when pilots are manipulated by hijackers or pilots intend to commit suicide, the airliner is dangerous. As a safer solution, BHUAP cannot be deployed in the airliner due to a few pressing challenges ranging from the single point of compromise for ATCs and the unreliable and

unsafe communication channel. In this paper, we propose a new framework to strength its security. Both the performance evaluation and the experiments results show that our novel framework for ATM are feasible, secure, and efficient.

ACKNOWLEDGEMENT

This work was supported in part by the US National Science Foundation under grants CNS-1422301 and CNS-1514014.

REFERENCES

[1] F. A. Administration. Chapter 2 human behavior. In *Risk Management Handbook. U.S. Department of Transportation. [Online]: http://www.faa.gov/library/manuals/aviation/*, pages 2.1–2.2, 2009.

[2] S. Ba and P. A. Pavlou. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS quarterly*, pages 243–268, 2002.

[3] H. Bai, M. Atiquzzaman, and D. Lilja. Wireless sensor network for aircraft health monitoring. In *Broadband Networks, 2004. BroadNets 2004. Proceedings. First International Conference on*, pages 748–750. IEEE, 2004.

[4] M. G. Ballin, J. M. Hoekstra, D. J. Wing, and G. Lohr. Nasa langley and nlr research of distributed air/ground traffic management. In *AIAA's Aircraft Technology, Integration, and Operations (ATIO) 2002 Technical Forum, Los Angeles, California, AIAA*, volume 5826, pages 1–3, 2002.

[5] R. Barhydt and A. W. Warren. *Development of intent information changes to revised minimum aviation system performance standards for automatic dependent surveillance broadcast (RTCA/DO-242A)*. Citeseer, 2002.

[6] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE, 2007.

[7] M. Blaum and R. M. Roth. New array codes for multiple phased burst correction. *Information Theory, IEEE Transactions on*, 39(1):66–77, 1993.

[8] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In *Advances in CryptologyASIACRYPT 2001*, pages 514–532. Springer, 2001.

[9] E. Brown, D. Cameron, K. Krothapalli, W. von Klein, and T. Williams. System and method for automatically controlling a path of travel of a vehicle, Nov. 28 2006. US Patent 7,142,971.

[10] M. X. Cheng and Y. J. Zhao. Connectivity of ad hoc networks for advanced air traffic management. *Journal of Aerospace Computing, Information, and Communication*, 1(5):225–238, 2004.

[11] A. Costin and A. Francillon. Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. *Black Hat USA*, 2012.

[12] R. M. Harman. Wireless solutions for aircraft condition based maintenance systems. In *Aerospace Conference Proceedings, 2002. IEEE*, volume 6, pages 6–2877. IEEE, 2002.

[13] M. Kamgarpour. Optimal control of hybrid systems in air traffic applications. 2011.

[14] D. Li and S. Sampalli. A hybrid group key management protocol for reliable and authenticated rekeying. *IJ Network Security*, 6(3):270–281, 2008.

[15] S. Miner and J. Staddon. Graph-based authentication of digital streams. In *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on*, pages 232–246. IEEE, 2001.

[16] A. A. S. Network. Aviation safety database. *[Online]:http://aviation-safety.net/database/*, 2015.

[17] B. News. Crash leaves many unanswered questions. *[Online]: URL:http://www.bbc.com/news/world-europe-32084956.*, 2015.

[18] B. News. Germanwings: Crash leaves many unanswered questions. *[Online]: URL:http://www.bbc.com/news/world-europe-32084956*, 2015.

[19] T. G. News. Revenge drove pilot to crash plane, killing 217. *[Online]: URL:http://www.theguardian.com/world/2002/mar*, 2002.

[20] T. C. of Federal Regulations. Electronic code of federal regulations - part 91 general operating and flight rules. *[Online]: http://www.ecfr.gov/*, 2015.

[21] I. C. A. Organization. Strong passenger results and a rebound for freight traffic in 2014. *[Online]:http://www.icao.int/Newsroom/Pages/Strong-Passenger-Results-and-a-Rebound.aspx.*, 2014.

[22] G. Pappas, C. Tomlin, J. Lygeros, D. Godbole, and S. Sastry. A next generation architecture for air traffic management systems. In *Decision and Control, 1997., Proceedings of the 36th IEEE Conference on*, volume 3, pages 2405–2410. IEEE, 1997.

[23] J. M. Park, E. K. Chong, and H. J. Siegel. Efficient multicast stream authentication using erasure codes. *ACM Transactions on Information and System Security (TISSEC)*, 6(2):258–285, 2003.

[24] M. O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM (JACM)*, 36(2):335–348, 1989.

[25] A. Roy. Secure aircraft communications addressing and reporting system (acars), Feb. 13 2003. US Patent App. 10/215,730.

[26] K. Sampigethaya, R. Poovendran, and L. Bushnell. Secure operation, control, and maintenance of future e-enabled airplanes. *Proceedings of the IEEE*, 96(12):1992–2007, 2008.

[27] E. Schrader. Cheney gave order to shoot down jets. *Los Angeles Times, [Online]: http://articles.latimes.com/2004/jun/18/nation/na-cheney18*, 2004.

[28] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[29] M. Strohmeier, M. Schfer, V. Lenders, and I. Martinovic. Realities and challenges of nextgen air traffic management: The case of ads-b. *Communications Magazine, IEEE*, 52(5):111–118, 2014.

[30] J. Todd and L. Yount. Flight control modules merged into the integrated modular avionics, Sept. 6 2002. WO Patent App. PCT/US2001/022,063.

[31] W. True, A. Malaga, M. Larsen, and R. Eckert. Aircraft data link network routing, Feb. 12 2009. US Patent App. 11/835,864.

[32] Y. Wang and Y. Desmedt. Efficient secret sharing schemes achieving optimal information rate. In *Information Theory Workshop (ITW), 2014 IEEE*, pages 516–520. IEEE, 2014.

[33] C. A. Wargo and C. Dhas. Security considerations for the e-enabled aircraft. In *IEEE Aerospace Conference*, 2003.

[34] W. Website. Ground proximity warning system. *[Online]: https://en.wikipedia.org/wiki/Ground-proximity-warning-system*, 1996.

[35] W. Website. Boeing honeywell uninterruptible autopilot. *[Online]: https://en.wikipedia.org/wiki/Boeing-Honeywell-Uninterruptible-Autopilot*, 2006.

[36] W. Website. Unmanned aerial vehicle. *[Online]: http://en.wikipedia.org/wiki/Unmanned-aerial-vehicle*, 2014.

[37] W. Website. Autopilot. *[Online]: https://en.wikipedia.org/wiki/Autopilot*, 2015.

[38] W. Website. September 11 attacks. *[Online] https://en.wikipedia.org/wiki/September-11-attacks*, 2015.

[39] M. Yajnik, S. Moon, J. Kurose, and D. Towsley. Measurement and modelling of the temporal dependence in packet loss. In *INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 1, pages 345–352. IEEE, 1999.

[40] L. Yount, J. Jackson, E. Christianson, and A. Beutler. Method and apparatus for preventing an unauthorized flight of an aircraft, Jan. 13 2009. US Patent 7,475,851.

[41] A. D. Zeitlin and R. C. Strain. Augmenting ads-b with traffic information service-broadcast. In *Digital Avionics Systems Conference, 2002. Proceedings. The 21st*, volume 1, pages 3D2–1. IEEE, 2002.

[42] W. Zhang, M. Kamgarpour, D. Sun, and C. J. Tomlin. A hierarchical flight planning framework for air traffic management. *Proceedings of the IEEE*, 100(1):179–194, 2012.