A Multi-Secret Value Access Control Framework for Airliner in Multinational Air Traffic Management

Depeng Li, Rui Zhang, Yingfei Dong, Fangjin Zhu and Dusko Pavlovic

***Abstract*—When been threatened by hijacking or suicide-by-pilots, the airliner may either crash itself or be shot down due to the potential of the suicide attack. There exist some solutions that allow air traffic controllers or federal agents to take over pilots' authority in the emergency. Though rarely, an air traffic controller may abuse this privilege to mishandle airliners that leads to catastrophic events. In this paper, to mitigate such risks, we propose a multi-secret value access control framework based on new designed and existing cryptographic techniques such as XOR-based secret sharing schemes. It not only satisfies the efficiency requirement but also assures that each nation owns a unique secret value. We further develop and implement the XOR-based secret sharing scheme on Linux system. Both the experimental results and performance evaluation demonstrate that our solution is not only efficient and bust also secure by design for the multinational air traffic management.**

***Index Terms*—Access Control, Air Traffic Control, Multi-Secret Value.**

I. Introduction

In the Internet of Things (IoT) ecosystem, an inherent synergy between cyber and physical functions cut across a massive number of co-exisiting devices. The tight coupling between the cyber and physical functions of each object could be utilized in a range of applications such as smart home [9], smart grids [23], [57], transportation [21], [26], and others [60], [18], [25]. However, a glaring obstacle to the widespread deployment of IoT is the security and safety concern [27], [22].

Safety is of paramount importance in aviation because a considerable number of lives are always at stake. According to the International Civil Aviation Organization (ICAO), about 3.2 billion passengers travel by commercial airliner in 2014 and the annual passenger number is expected to be 6.4 billion by 2030 [39]. However, flying involves risks: as one of the most terrifying risks, hijacking or suicide-by-pilot [32] not only kills the persons on board but also results in suicide attacks, i.e., massacring people on the ground. As an example, in the September 11 attack, 265 persons aboard were killed by hijacking, and the subsequent suicide attacks also claimed 2,731 lives on the ground.

Current flight control systems face several pilot-related risks. First, hijackers on board may manipulate pilots. For example, on September 11, 2001, terrorists hijacked four airliners and carried out suicide attacks. Moreover, pilots may deliberately crash an airliner. For example, in 2015, Andreas Lubitz, the co-pilot, overrode auto-pilots' privilege and flew Germanwings Flight 4U 9525 into a mountain committing murder-suicide [34]. Furthermore, pilots can operate the airliner contrary to air traffic control operator (in short, ATC)'s instructions, but ATCs cannot enforce their wills on pilots.

So far, there are several means to handle hijacked airplanes. First, as one of the most frequently used solutions, shooting down aircraft could avoid suicide attacks. For example, 109 hijacked aircraft have been shot down in the last three decades [32]. In particular, on September 11, 2001, Vice President Cheney issued an order to shoot down hijacked airliners [46]. Second, to better mitigate pilot-related risks, Boeing and Honeywell introduced a patent, the Boeing Honeywell Uninterruptible Autopilot (BHUAP) [54] to take over pilots' authority by ATC or federal agents in emergencies. 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) [48] [12]). The communication channel links the air traffic control stations on the ground and the e-enabled airplane [59]. Once the mode is activated, nobody can turn it off, and the airliner will be landed automatically at a nearby airport. It benefits from advanced technologies in both the aviation and the air traffic management (ATM) systems: the integration of aviation communication technologies, e-enabled airplanes [44], and the remote control technology.

However, the airlines and the pilot union cannot support BHUAP without carefully addressing a critical challenge, which is the abuse of privileges by ATCs or Federal Agents [35].

- *Single point of compromise of ATC*: With the purpose of reducing the risk of the single point of compromise of pilots, ATCs are granted the privilege to take over pilots' control right via BHUAP. However, an ATC may also become the single point of compromise in certain situation;
- *ATCs for Airliner*: While an airliner flies across different countries, ATCs from the relevant country should monitor and guide it. How to assign the appropriate access privilege

D. Li and D. Pavlovic are with the Department of Information and Computer Sciences, University of Hawaii at Manoa, Honolulu, HI, 96822 USA (e-mail: depengli@hawaii.edu, dusko@hawaii.edu).

R. Zhang is with the Department of Computer and Information Sciences, University of Delaware, Newark, DE, 19716 USA (e-mail: ruizhang@udel.edu).

Y. Dong is with the Department of Electrical and Computer Engineering, University of Hawaii at Manoa, Honolulu, HI, 96822 USA (e-mail: yingfei@hawaii.edu).

F. Zhu is with the College of Computer Science and Technology, Shandong University, Jinan, Shandong, 250014 China (e-mail: zhufj@sdu.edu.cn).

Manuscript received XX/XX, XXXX

to those ATCs is also a difficult challenge;

In this paper, we introduce a new multi-secret value access control framework for ATM to mitigate the security risks resulted from the BHUAP system. To the best of our knowledge, we are the first to address above challenges.

Our framework is composed of the following components:

(A) *Efficient Threshold-based Access Control Mechanism*: When an ATC takes over pilots' authority by activating the BHUAP, it is possible that the ATC is compromised or the ATC's credential is stolen. To prevent the single point of compromise, we construct a *(t, n)* threshold access control mechanism that prevents one single compromised ATC from manipulating the pilots' privilege by leveraging the XOR-operation secret sharing scheme [51]. Meanwhile, considering that the air traffic management is a time-critical application, our solution provides computational efficiency.

(B) *Trust-based, Unequal Secret Sharing Scheme and Trust Evaluation System*: there may be less than t ATCs on service for a traditional (t, n) threshold access control method. To handle this scenario, we further propose the trust-based, unequal secret sharing method and design a trust evaluation system to estimate the trust value of each ATC.

(C) *Unique Secret Value for Authority of Each Country*: Regarding an airliner flying across multiple countries, a single secret value access control mechanism is not applicable, considering that authorities of different countries (countries, in short) should have different secret values. We further propose the multi-secret value threshold-based access control scheme.

In our previous conference version [24], we studied the security and reliability issues of digital communication channels as well as access control issues. To address the pressing concerns, we propose a framework with the main focus on a Reliable and Authenticated Protocol (RAP) which enhances the communication reliability and offer the authentication service. More importantly, two threshold-based access control schemes, one is the efficient-oriented and the other the attribute-oriented, have been proposed to mitigate the single point of compromise problem. This journal paper mainly targets on a particular scenario in which an airliner flies across multi countries. The single point of compromise problem is much more complicated considering that each country is deemed to be in charge of its own air traffic management service. This is because that this issue deeply impacts the national security.

Compared with the previous conference version [24], this paper makes four key contributions concerning the access control framework. First, we propose an efficient access control framework which integrates a series of schemes to solve the single point of compromise problem. This includes the assessment of the critical trust system and the providence of efficiency service, both of which are important for air traffic management for every country. We propose In particular a multi-secret value access control framework which can supply one secret value for each country where the airliner flies across. Considering that our previous conference version [24] only equips one single secret value for all countries, the new solution renders enhanced security. Second, we design a specific trust value evaluation system to gauge the trust value for each ATC based on practical tracks of history. Compared with the standard trust evaluation means in our conference version, it is more feasible. Third, the threshold-based access control scheme introduced in this paper is solely based on bitwise XOR operations but in our previous conference version [24] the access control system involves some other expensive operations such as polynomial equation calculations and even the Elliptic Curve Pairing operations. Finally, we develop and implement a software package based on Linux OS through invoking the Schifra ECC library [45] and GNU GPL library. Experiments have been conducted to validate the efficiency of the proposed access control system.

II. Background

A. Symbol Table

A_j	an ATC
$\mathbb{A}$	a set of ATCs
A_i^j	the n^j ATCs in its own country T^j
$\mathbb{A}^j$	the set of ATC in country A^j
c	a codeword
C	a Matrix
c_j	an entry
c_i^j	ATC A_i^j's secret sharing for country T^j
Cr_j	a credential associated with ATC A_j
$CF(A)$	the trust value assigned to ATC A
$CR(x)$	ATC x's credit score
CS_j	control server of country T^j
CKS	the central key server
$f(z)$	the other polynomial with degree $t-1$
f_A	the number of flights an ATC A had monitored
F	general finite field
$gcd(p,q)$	greatest common divisor of integers p and q if $gcd(p,q)=1$, it means p and q are mutually prime
$g(z)$	the generator polynomial over $F=GF(q^m)$ for the Reed-Solomon code
H	Hash Function
$\mathbf{H}$	$r \times p$ matrix
K	Key, a randomly generated value
$\mathbf{M}$	a $(p-1)\times(n+1)$ matrix over $F=GF(q)$
MS	the master secret value which is used as a seed to generate the secret value of each country
$N_p(x)$	a polynomial
$p(A,i)$	at the i^{th} flight, P is another ATC working with A
P_i	pilot i
R_p	the rings of $N_p(x)$
S	a secret value defined as a sequence of binary numbers
S^j	the secret value for each country T^j
$S(A,i)$	the rating that P gives to A
T^j	the j^{th} Country
$\mathbb{T}$	a set of countries
$TF(A,i)$	the trust value for flight i
V_i^j	the trust value for ATC A_i^j
(t',t)	t': the least threshold value, t: the threshold value
(t,n)	Threshold Access Control
(t^j,n^j)	threshold-based access control pair for the j^{th} Country
t_{min}^j	the minimum number of ATCs online for country T^j
$R(A_x^y)$	the trust value of an ATC who serves the country T^y
α	a root for $N_p(x)$ in ring R_p
Γ	a matrix
μ	he trust weight that others measure an ATC A
ν	the trust weight the system measure an ATC A
τ	$\tau=\|S\|$, the length of secret value

Table I: Table of Notations

B. Brief Introduction of Aviation System

1) Air Traffic Management (ATM): With the continuous growth of the air traffic demand and the security requirement, the paradigm shift from traditional ATM to the advanced system is necessary. In detail, the ground-based navigation system is replaced with the satellite-based communication system, the verbal communication and ground radar system is switched to more accurate and reliable digital communications, and the traditional aircraft is substituted for e-enabled ones. Therefore, the modern, underway ATM system could accommodate much more aviation applications such as safety decision-making systems [19], conflict detection and resolution, and 4D trajectory based operations [44]. In summary, the current ATM system incorporates the sophisticated sensing and monitoring technologies enabled by more reliable digital communications with real-time situational awareness for both pilots and ATCs [19] [62].

2) Flight Control System: The flight control system interleaves between a pilot and an auto-fly pilot (autopilot, in short) [56]. The pilot is the final authority for the safety operation of the commercial airliner. A pilot supervises the auto-pilot system and can override the auto-pilot when necessary. Meanwhile, pilots should comply with the ATC who oversees the area. In an emergency that requires immediate actions, pilots can deviate from ATCs' instructions to the extent which is necessary to meet the emergency [37]. 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-related behaviors [2], which include both hijackings and suicidal flights that happened 369 and 19 times since 1985, respectively [32].

3) Wireless communication for aviation - Boeing Communication and ADS-B: (1) *Boeing*: with the purpose to enable remote access of ATCs for an airliner via the cyber communication channel, Boeing airplanes leverage the existing data communication methods. Remote ATCs could communicate with airliners via radio or satellite communication channels [16] [55]. In detail, the Aircraft Communication Addressing and Reporting System (ACARS) can transmit data between the Flight Management System (FMS) of airliners and ground stations (e.g. airports, aircraft maintenance bases, air traffic control towers and so on) via radio and satellite technologies [43]. The aircraft data link network routing technology [50] could provide packet routing function [3]. To ensure security, BHUAP invokes aircraft specific encryption keys in ATC/military or other aviation carriers. Thus, the *e-enabled airliner* [44] could be connected with a global information network [52] with the protection of security services. (2) *ADS-B*: ADS-B is developed to replace the traditional radar-based system. ADS-B broadcasts messages over radio transmission links within almost every 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, and messages are encoded with the block size as 56 bits or 112 bits [12].

4) E-enabled air traffic control: Air traffic control systems are developed to transmit critical information between ground ATCs and e-enabled airplanes [44]. The airplane periodically broadcasts [11] identities, accurate states (e.g., position, altitude, speed, etc.), and other messages (e.g., waypoints) to ground ATCs [40]. ATCs can issue tasks and other airplanes' situation awareness information to pilots [5] [61]. This information could be used by ATC to analyze the airliner's states and could also be shared with other airliners [4].

5) BHUAP system to activate taking-over button: BHUAP is designed to prevent hijacking. Generally, in an airliner, 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 pilots keep on ignoring this alarm, ATCs could trigger the BHUAP mode remotely. It is difficult to switch off BHUAP since BHUAP connects with a separate independent power supply system. This method prevents the compromised pilots or hijackers from turning off the crash warning system or BHUAP [49].

III. Related Work

A. Secret Sharing Schemes (SSS)

Secret sharing schemes are well applied in the access control of information systems, e.g., distributed networks. However, to the best of our knowledge, secret sharing schemes have not been popularly deployed in either aviation systems or air traffic control systems. The reason is that the aviation system highly demands efficiency. But traditional secret sharing schemes relies on the Galois field and therefore is computational expensive. In subsubsections 1), 2) and 3), we describe the secret sharing schemes in which we concentrate on performance. Then, we explain the secret sharing schemes with the focus on information rate:

Performance of Secret Sharing Schemes:

1) Shamir's (t,n) threshold scheme: Shamir's *(t,n)* threshold scheme [47] is based on Lagrange interpolation to ensure the secret recovery with the shares of any k out of n participants.

- *Setup Phase*: Setup phase of our secret sharing system will, based on key K, compute $k_1, ..., k_n$ in which $k_i = f(i) mod\ p$ where p is a prime and $f(x)$ is an unknown polynomial of degree less than t given by the Lagrange interpolation formula (1). Each k_i, where $1 \leq i \leq (t)$ is distributed to a corresponding ATC one by one via secure channels. The coefficients of $f(x)$, namely, $a_1, ..., a_{t-1}$ are randomly generated independent values but $a_0 = K$. Also, (x_i, y_i), are points to define $f(x)$ where $1 \leq i \leq t$.
- *Pooling of shares phase*: it requires any group of t or more ATCs to, through secure channels, contribute their distinct shares (i, k_i) which are treated as (x_i, y_i). The key K is recovered by formula (2):

$$f(x) = \sum_{i=1}^{t} (y_i) \prod_{i=1, i \neq j}^{t} \frac{(x - x_j)}{(x_i - x_j)} \tag{1}$$

$$K = a_0 = f(0) = \sum_{i=1}^{t} (y_i) \prod_{i=1, i \neq j}^{t} \frac{(x_j)}{(x_i - x_j)} \quad (2)$$

2) Secret Sharing Schemes based on Reed-Solomon codes: The secret sharing scheme based on Reed-Solomon codes has been developed in [29]. It takes *O(nlogn)* field operations in the secret distribution phase and $O(n^2)$ in the secret reconstruction phase.

3) Secret Sharing Schemes based on XOR operations: To reduce the aforementioned expensive computational cost, some special, fast *(2,n) and (3,n)* threshold schemes [17], [31] based on XOR or additive operations has been proposed. In [20], [28], in sake of high performance, the generalized *(k,n)* threshold scheme is proposed to extend the number of participants from 2 or 3 to k by using just EXCLUSIVE-OR(XOR) operations. In these schemes, faster computation to split shares and reconstruct the secret has been achieved as compared with other kinds of SSS schemes. Furthermore, the information leak regarding the secret cannot be realized. Meanwhile, the bit-size of each share is as same as that of the secret of Shamir's scheme. Especially, to recover the secret, these schemes concatenate *XORed* terms of a divided piece of the secret and a random number with the properties of prime numbers. Consequently, these *XORed* terms will be specifically circulated in a pattern so that they do not overlap with each other.

Communication Overhead of Secret Sharing Schemes: To reduce the communication overhead, a few information rate-saving SSS schemes have been developed based on Block Code: In [14], a block-box secret sharing scheme has been proposed. In this scheme, the secret and the shares are selected in a group G. But the distribution matrix and the reconstruction vectors are defined over integer rings Z. The information rate of this scheme is n in this (n, k) black-box threshold secret sharing scheme. In [13], a new (n, k) black-box threshold SSS scheme over general Abelian group is proposed with the optimized lower bound $O(log_2 n)$. A specific technique utilizing a pair of $l \times l$ Vandermonde matrices together with co-prime determinants are developed to design low degree integral extensions of the integer ring Z.

B. Security and Safety Mechanism on Aviation and IoT System

Cyber-physical systems are envisioned to transform the way engineered system functions, by relying on joint functioning of information systems and physical components. These IoT-enabled CPS systems are already replacing existing infrastructures such as the electricity grid, air traffic management, and advanced manufacturing. However, cyber communication that is essential to drive this progress is far from being truly secure [27], [22]. In [9], a real-world smart home system, namely, digital-Storm, is analyzed. A variety of attack vectors or entry points into a smart home system are ranked in order to propose solutions to remedy or diminish the risk. In [23], the possible sensitive information leakages and potential privacy threats in the automatic appliance control (AAC) application of smart grids are analyzed. An attribute-based encryption (ABE) key management variant is proposed to provide fine-grained privacy preservation. In [57], to better evaluate the effectiveness while integrating distributed energy resources and storage devices, a theoretical framework that can model and analyze three types of power grid systems is proposed. In [21], the critical operations which could potentially crash the airliner have been studied. An efficient, authenticated, secure solution are proposed so that the air traffic controller may intervene or even to prohibit the critical but dangerous operations. In [26], a Dynamic En-route Decision real-time Route guidance (DEDR) scheme is proposed. There are two folds, one is to effectively lower road congestion which is resulted from the sudden increase of vehicles and the other to mitigate the travel time as well as the fuel consumption. In [60], Ultra Dense Networks (UDN) are studied. A taxonomy to review and describe existing research efforts is developed and a few criteria such as, handover performance, energy efficiency and others are analyzed. Other researches related with privacy [25] and key agreement [18] have been studied to explore feasible and efficient protection solutions.

After the tragedy of 9/11, one of the new Federal Aviation Administration (FAA) safety rules requires that cockpit doors be closed and locked during flight except for brief pilot breaks, such as to visit the bathroom. To comply with the FAA's new requirement, operators of commercial airlines also harden their airplanes' cockpit doors to withstand intruders, small arms fire, and even some grenades [38]. The cockpit door is supposed to be the last line of defense from outside aggressors.

However, airlines have fewer options if threats come from within the cockpit: In the accident of Germanwings Flight 4U 9525, after successfully locking the plane's pilot out of the cockpit, Andreas Lubitz took advantage of the cockpit door access mechanism - designed after 9/11 for the event of terrorist emergence - which allows someone in the cockpit to override the coded entry mechanism on the outside of the door. This time, the cockpit safety mechanism was misused to bar the captain instead of terrorists. Shortly after Germanwings Flight's crash, a few international airlines announced the adoption of the so-called "two-person cockpit rule" - a U.S. federal requirement enforced for several years in the U.S. - which mandates a second crew member being in the cockpit at all times. But there are still some concerns, (1) it is possible that the "two persons" conspire a suicide flight, though its possibility is lower than that of only one pilot. (2) The temporary crew member may possibly be fooled by rogue pilots due to a lack of sufficient flight experience. Or one pilot could be knocked out by the other one who intends to maliciously take over the flight controls. . In the Egypt Air flight 990 accident in 1999, Gamil el-Batouty switched off the auto-pilot and shut down the fuel to both engines. While initially out of the cockpit, Captain Ahmed el-Habashi managed to struggle back in, fought against Gamil, grabbed the controls and pulled the airplane up. However, the airplane crashed due to loss of all power and distraction of Gamil [36]. These are other occasions where

human pilots commit murder-suicide: Malaysia Airlines flight MH370 in 2014 [41], LAM Flight TM-470 in 2013 [33], etc. The FAA released a study in 2014 indicating that, from 2003 to 2012, eight accidents were determined to be suicides [15].

Since the human pilot can make mistakes, after 9/11 people investigated the possibility of the control tower wresting control of an airliner through cyber communication channels. The remotely controlled drone indicates that the required technology is already mature: remote ATCs could communicate with aircraft via radio or satellite communication channels [55]. BHUAP also demonstrates that it is ready to transfer PIC's authority to ATCs [30]. To ensure security, BHUAP invokes an aircraft specific encryption key in ATC/military or other aviation carriers [10]. However, both pilots and airlines still reject to utilize this new Boeing and Honeywell technology [30] due to cyber security, specifically the access control scheme.

To enable remote control of an airliner from ATCs via cyber communication channel, both data communication and data link network routing are available. The Aircraft Communication Addressing and Reporting System (ACARS) via radio and satellite technology can transmit data between the Flight Management System (FMS) of airliners and ground stations (airports, aircraft maintenance bases, air traffic control, etc.) [43]. Aircraft data link network routing technology [50], for example, could provide packet routing function.

Utilizing BHUAP Alarms to Activate Taking-Over Button - Since the human pilot can make mistakes, after 9/11 people investigated the possibility of the control tower wresting control of an airliner through cyber communication channels. In the BHUAP system [10], [59], a crash-warning device, which is already common on any airliners, connects with cockpit computers. This prevents the airliner from crashing into obstacles. When hijackers force the PICs to crash the airliner or PICs themselves deliberately to do so, audible warnings from crash-avoidance systems are triggered. If PICs keep on ignoring this alarm, ATCs could take over PICs' authority since PICs do not care about the airliner safety. However, the compromised PICs or the hijackers may turn off the crash warning system. To prevent this from happening, the BHUAP already uses the Flight Control Computer (FCM) which is connected to a separate power supply and its purpose is to add redundancy to the system [49]. Thus, Airplane Information Management System (AIMS), autopilots, Navigational FCM are all directly connected to the Actuator Control Electronics (ACE) system and they all have independent power supplies. AIMS could now coordinate all flight control functions with no need of the cockpit. Even if everything in the cockpit turns off, AIMS can still function normally, either through executing a pre-programmed flight plan or by opening an RF data link to an external source in order to receive direct instructions. Therefore, compromised PICs or hijackers who occupy the cockpit, still cannot totally control the BHUAP as well as the crash-warning device which have both their own power supply and preprogrammed management system. So, ATCs can take the chance to activate the button withdrawing PICs or hijacker's authority. However, the problem of this alarm system is that it only can function in the last a few minute and there is a high possibility that the airliner will crash since the left time is not sufficient to rescue the airliner.

IV. Problem Formulation and Threat Model

A. Introduction

The air traffic control system consists of six components. They are (i) E-enabled airliners, (ii) Two kinds of users, pilots and ATCs, (iii) Air traffic control computers which are used by ATCs, located in air traffic control stations, and connected with each other via network systems, (iv) Central key server which generates secret values for each nation, calculates corresponding secret shares, and distributes these shares to ATCs, (v) Control server which is located in the air traffic control station and its function is to reconstruct the secret value that is used as a key to encrypt control instructions (i.e., to activate BHUAP button), and (vi) Wireless digital communication network (e.g., Boeing or ADS-B) connecting control servers and airliners.

In this paper, we assume that the airliner has already deployed two devices (a) BHUAP device and (b) ground proximity warning system (GPWS) [53]. The former is embedded within pre-programmed firmware in an airliner. Its function is to disable/override the pilot's operating authority on board. The latter triggers the alarm when the crashing risk is detected. In detail, an ATC who works in the air traffic control station could be aware of a pilot's malicious operations. The other scenario is that when the GPWS triggers the alarm, the pilot keeps ignoring the audible warnings. At both scenarios, the ATC could execute the privilege to take over the pilot's authority. The control instruction to activate BHUAP button is forwarded from the control server (CS) to the airliner through Boeing / ADS-B communication channels.

B. Problem Formulation

An ATC is denoted by $A_j \in \mathbb{A} = \{A_1, A_2, ..., A_n\}$ *where* $1 \leq j \leq n$ and $\mathbb{A}$ is a set of ATCs. Each ATC A_j is associated with a credential Cr_j. By using Cr_j, 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.

However, compromised ATCs could threaten airliner's safety through mishandling access rights to withdraw pilots' authority. If any ATC could activate the BHUAP button to take away pilots' privilege, the airliner's safety is at the risk of the single point of compromise. The reason lays in the fact that any ATC may act maliciously. Here are a few scenarios: (1) A malicious ATC A_j Charlie could withdraw pilots P_i's authority whenever A_j logins and accesses an ATC computer by inputting the user account and credential Cr_j. (2) An 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 mentioned above could also happen for ATCs who has a high rank. (4) For an airliner flying across multiple countries, the relevant ATC should be assigned the privilege to activate the BHUAP button when and only when the airliner flies across his/her country. If the access right is assigned incorrectly, the BHUAP maybe misused. 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 relatively limited.

C. Threat Model

Both pilots and ATCs could act maliciously. In our threat model, we assume the followings:

(1) It is possible that the compromised pilot operates the airliner. A compromised ATC may also use the PC of the air traffic management system in a dangerous way. That is due to some potential causes including psychological issues (e.g., suicide), health problems (e.g. heart attack), and being threatened by other persons (e.g., terrorists, gangster).

(2) A malicious pilot P_{bad} can mislead, fool, or attack his/her colleagues in the cockpit. Thus, it 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 somewhere else.

(3) A malicious ATC could misuse the taking over privilege on air traffic management PC to activate BHUAP function.

(4) It is hard for the pilot or the ATC to break modern cryptographic primitives such as threshold secret sharing, keyed hash functions, etc.

(5) Devices within the airliners or PC in air traffic management station are tamper-resistant so that nobody can either compromise them or extract cryptographic keys stored in them.

D. Goals, Scope, Assumptions, and Limits

Goals: This paper attempts to propose a set of solutions which could mitigate the risk that malicious pilots/ATCs, P_i/A_j access the BHUAP button of an airliner fling across multiple countries. With the purpose to achieve this goal, the proposed counteraction should satisfy the following security requirements *(i) threshold access control for BHUAP*: to provide a threshold access control mechanism restricting the absolute privilege of one single ATC. *(ii) resilience for lack of t ATCs*: to present a flexible solution while the lack of enough ATCs, and *(iii) efficiency*, due to the real-time requirement and the increase of traffic demands, the proposed solution should be efficient.

Assumption: Like other research in security areas, we assume that (1) the majority of ATCs (particularly, t out of n) are honest and trustful. (2) We also assume that devices in the airliner such as BHUAP, GPWS are tamper-resistant. (3) Device attestations are assumed to be deployed on the airliner to validate devices on board. (4) We assume the existence of the reliable and authenticated communication channel between ATC stations and e-enabled airliners.

Limits: Since just focusing on restricting ATCs A_j's privilege of overriding pilots' authority, this paper can mitigate but cannot eliminate risks introduced by malicious ATCs. Furthermore, some other existing risks, e.g., wireless communication interference will not be comprehensively studied and addressed.

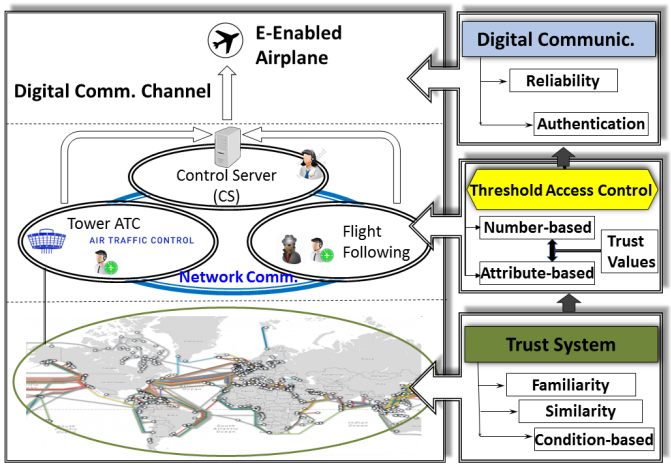

Fig. 1: System Architecture

Scope and Future Works: There are some interesting problems will not be considered in this paper, but we hope that they may inspire other researchers. (1) Why ATCs/pilots could be compromised and how to handle this problem? (2) How to promptly detect the hijacking or the suicide-by-pilot? (3) 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. (4) ADS-B / Boeing communication channels may be targeted by hackers who launch attacks such as Denial of Service (DoS) attacks, radio interference attacks, etc. How to counteract them? (5) Since the (t, n) threshold-based secret sharing is adapted to fit in our solution, how to determine the actual value for both t and n is critical, but they cannot be decided until a practical field test of the implementation of threshold-based access control in the aviation system.

V. Access Control Mechanism with Multi Secret Values

In this section, we first describe the proposed system architecture which is composed of three layers. Then, we introduce the proposed solution consisting of five phases: (1) system initialization, (2) generation of the chain of secret values, (3) multi-secret values and the key management, (4) trust-based, unequal, XOR-operation secret sharing, and (5) trust evaluation engine and secret value recovery.

A. System Architecture

As depicted in Fig. 1, the proposed system architecture consists of three layers:

(1) Trust system layer: We develop a 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.

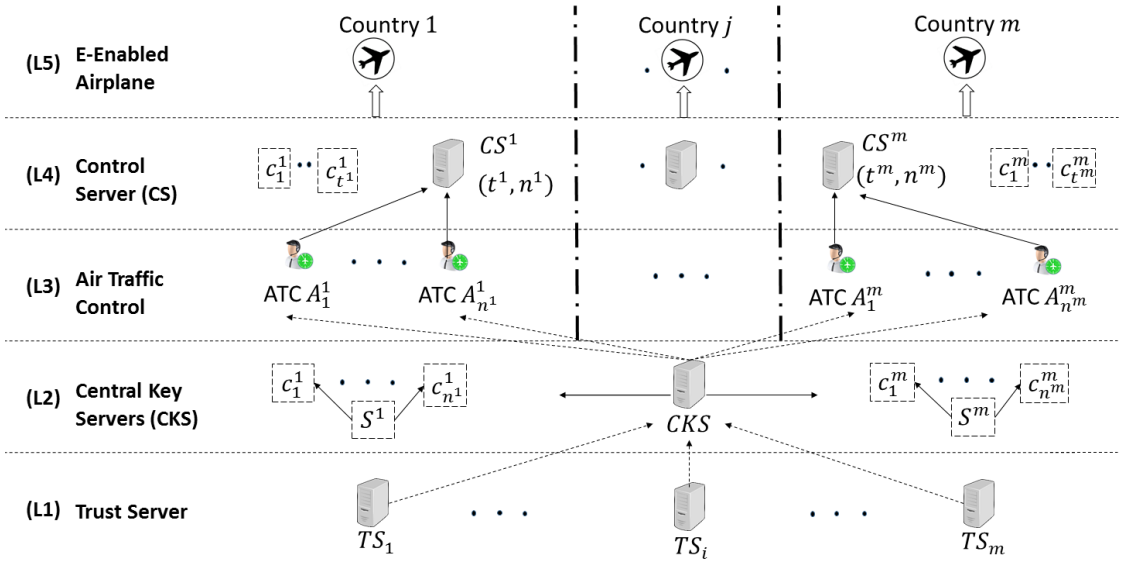

Fig. 2: Proposed System Model

(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, *(a)* we deploy an XOR-operation threshold access control [51] to achieve the (t, n) threshold access control goal. Both the secret share distribution and the secret share recovery are provided. *(b)* for an airliner, we propose multi-secert value means to enhance our secret sharing scheme in such a way that t out of n ATCs from the same country could reconstruct the secret value corresponding to this given country. *(c)* however, the secret share, sometimes, cannot be restored due to the lack of t ATCs online. We further address the challenge via trust-based, unequal, secret sharing scheme.

(3) Digital Communication Layer: In this layer, the control instruction is protected and delivered from the control server to the e-enabled airplane via digital communication channels (e.g. Boeing / ADS-B [48]). The reliability and authentication services should be provided for the communication but how to achieve the goal is out of the scope of this paper. At last, the e-enabled airplane (e-airplane) could receive the encrypted instructions sent from the control server. After decrypting the ciphertext, the e-airplane activates the BHUAP button.

Note that the layers in Fig. 1 and those in Fig.2 are closely related with each other. The map is that the "Digital Communication layer" in Fig. 1 corresponds to the "L5 E-enabled Airplane layer" in Fig.2, the "Trust System layer" in Fig. 1 to "L1 Trust Server layer" in Fig. 2, and the "Threshold-based access control in air traffic control layer" in Fig. 1 to the integration of L2, L3, and L4 layers in Fig. 2.

B. Overview of Proposed Solution

Although there exist some access control schemes [58], they are proposed for other distributed systems such as multiauthority cloud storage systems. Since the main challenges of the airliners concerning the air traffic control system are the efficiency and multi-secret values, we cannot adopt the existing access control schemes. Specifically, to design an access control framework for the BHUAP activation of an airliner, the most challenging issue is, when an e-enabled airliner flies across different countries, how to enable the secret value synchronization between the airliner and the control server in the related country. The second demanding request is that the proposed access control system should satisfy the time-critical requirement of the air traffic control system. The next challenge is to meet the resilience demand for threshold-based access control scheme.

We first describe the roles in our solution and the interactions between them. As depicted in Fig. 2, there are five layers which are explained from L5 to L1 below.

(1) at layer L5, we assume that the airliner L will fly across m countries, which are denoted by $T^j \in \mathbb{T} = \{T^1, T^2, ..., T^m\}$ *where* $1 \leq j \leq m$ and $\mathbb{T}$ is a set of countries.

(2) at layer L4, in each country T^j, there exists one control server CS_j in which the (t^j, n^j) threshold-based access control scheme is deployed.

(3) at layer L3, each of the n^j ATCs in its own country T^j is defined as $A_i^j \in \mathbb{A}^j = \{A_1^j, A_2^j, ..., A_{n^j}^j\}$ *where* $1 \leq i \leq n^j$.

(4) at layer L2, the central key server, CKS, will generate the master secret value MS, which is used as a seed to generate the secret value of each country. Based on MS, the CKS calculates the secret value S^j for each country T^j one by one. Refer to Algorithm 1 for the detailed method. Utilizing both the master secret value MS and the secret value S^j, the CKS computes $\{c_1^j, ..., c_i^j, ..., c_{n^j}^j\}$ and distributes each ATC A_i^j a secret sharing c_i^j for each country T^j. The CKS keeps on this operation till each ATC A_x^y at all countries has been assigned his/her secret sharing c_x^y *where* $\forall y \in [1, m]$ we have $x \in [1, n^y]$.

(5) at layer L1, the CKS retrieves the trust value V_i^j for each ATC A_i^j which has been calculated by a trust engine. Note that, to satisfy the requirements of this access traffic control system, we propose a trust engine in Section V (F) which models the assessment and the calculation of each pilot's trust value.

C. System Initialization

This phase includes three steps, CS setup, CKS setup, and TS setup.

(1) *CS setup*: the CS of each country executes its own CS setup algorithm to generate the threshold value t and the total value n of ATCs for that country. In detail, for each country $T^j \in \mathbb{T} = \{T^1, T^2, ..., T^n\}$ *where* $1 \leq j \leq m$, the CS setup algorithm let each country T^j input its threshold value (t^j, n^j). Then, the set of threshold values i.e. $\{(t^1, n^1), ...(t^j, n^j), ...(t^m, n^m)\}$ will be delivered to the CKS via secure communication channel.

ATC Registration: first, CS for each country T^j, namely, CS^j *where* $1 \leq j \leq m$ should register itself to CKS. In return, CKS should issue an unique id, namely cid to CS^j. Second, every ATC A_i^j of country T^j should register itself to their country's CS, namely, CS^j. In return, CS^j will issue A_i^j (a user) a pair of id (uid, cid), where uid is the user id and cid is the country id. In both steps, the id information should be delivered via authenticated channels.

(2) *CKS setup*: the CKS executes the CKS setup algorithm to generate a set of security parameters. First, CKS generates a random number $\alpha \in \mathbb{Z}_p$ and assign the master secret value $MS = \alpha$. Second, the CKS will initialize a sequence of secret values i.e. $[S^1, S^2, ..., S^m]$ for each country T^j *where* $j \in [1, m]$, respectively. Third, based on MS, a keyed hash function denoted by H is used to generate $[S^1, S^2, ..., S^m]$ with a key K, a randomly generated value *where* $K \in \mathbb{Z}_p$.

ATC Registration: first, CKS should respond the request from each country's CS, CS^j with the country id, cid, a randomly generated string. Second, for each country T^j, its CS CS^j should deliver all its ATC information to the CKS. Both communication should be protected via secure channels.

(3) *TS setup*: the TS executes the TS setup algorithm which first initializes the trust value for each ATC at each country. In detail, for each ATC A_x^y in each country $T^j \in \mathbb{T} = \{T^1, T^2, ..., T^n\}$ *where* $1 \leq j \leq m$, the TS setup algorithm let its trust value be $TR_x^y = 0$ and then calculate the trust value via the proposed trust engine.

ATC Registration: each ATC A_x^y should request to register at TS which will generate a corresponding record in its trust table.

D. Generation of the Chain of Secret Values for CKS

The CKS generates a sequence of secret values i.e. $[S^1, S^2, ..., S^m]$ which are, then assigned to corresponding countries $[T^1, T^2, ..., T^m]$ one by one.

The basic idea of our scheme is to utilize the DES-MAC algorithm to output a chain of secret values $[S^1, S^2, ..., S^m]$. The reason to invoke DES is due to its high security level. The DES-MAC algorithm should input two parameters, a key K and a string x which is a randomly generated string with the length $n * m$ *where* n is the block cipher E's length and m is the number of countries. When DES is used as the block cipher E, we let n = 64 in what follows, and the MAC key is a 56-bit DES key. In detail,

Algorithm 1 Algorithm GenerationSecretSharing

INPUT: data x, block cipher: DES, secret key: K for DES;
OUTPUT: m Secret Values based on x *where* |secret value|=n;
▷ x should satisfy $n(m-1) \leq \mid x \mid \leq nm$;
▷ *where* m: the number of countries;
▷ n: the block length of *DES*;

1: *Padding and blocking*. Divide the padded text x into n-bit blocks denoted as $x_1, ..., x_m$.
2: *DES processing*. Letting DES_k denote encryption using DES with key K, compute the block S^t as follows:
3: (1) $S^1 \leftarrow DES_k(MS)$
4: ▷ MS is the master secret value generated by CKS
5: (2) $S^i \leftarrow DES_k(S^{i-1} \oplus x_i)$ *where* $2 \leq i \leq m$.
6: *Completion*. The Secret values are the m blocks of $[S^1, S^2, ..., S^m]$ and each S_t is n-bit. If NOT successful, return result =1; else return result =0

E. Multi-Secret Values and Key Management

As illuminated in Fig. 3, our multi-secret value secret sharing scheme includes four steps, (1) Generation of secret sharings for each secret value, (2) Distribution of secret sharings, (3) recovery of secret values, and (4) Forwarding control commands to e-enabled airliners. The details are listed below:

(a) To distribute a unique secret value for each country: for an airliner which flies across m countries, each country T^j should be assigned a secret value $S^j \in S$ which could not be deduced by other countries. To satisfying this requirement, as described in section IV (C), the central key server CKS in our architecture generates a secret value MS and a key K. Based on both inputs, the CKS utilizes *Algorithm 1 GenerationSecretSharing* in section IV (D) to generate the chain of secret values $[S^1, S^2, ..., S^m]$ which will be used to compute the set of secret shares for each country T^j one by one.

Meanwhile, the CKS will forward the chain of secret values $[S^1, S^2, ..., S^m]$ to the e-airliner. When the e-airliner flies across country T^j, the key of BHUAP device will be replaced with the secret value S^j. The goal is to achieve the synchronization of both keys in the e-airliner and the control server CS at the ground.

(b) Distribution of secret sharings and recovery of a secret value in one country will be described in section IV (F).

(c) At country T^j, the control commands will be encrypted with the secret value S^j and the ciphertext will be forwarded to the e-airliner. After receiving the ciphertext, the e-airliner will decrypt it by using the corresponding secret value S^j since it is flying over the country T^j.

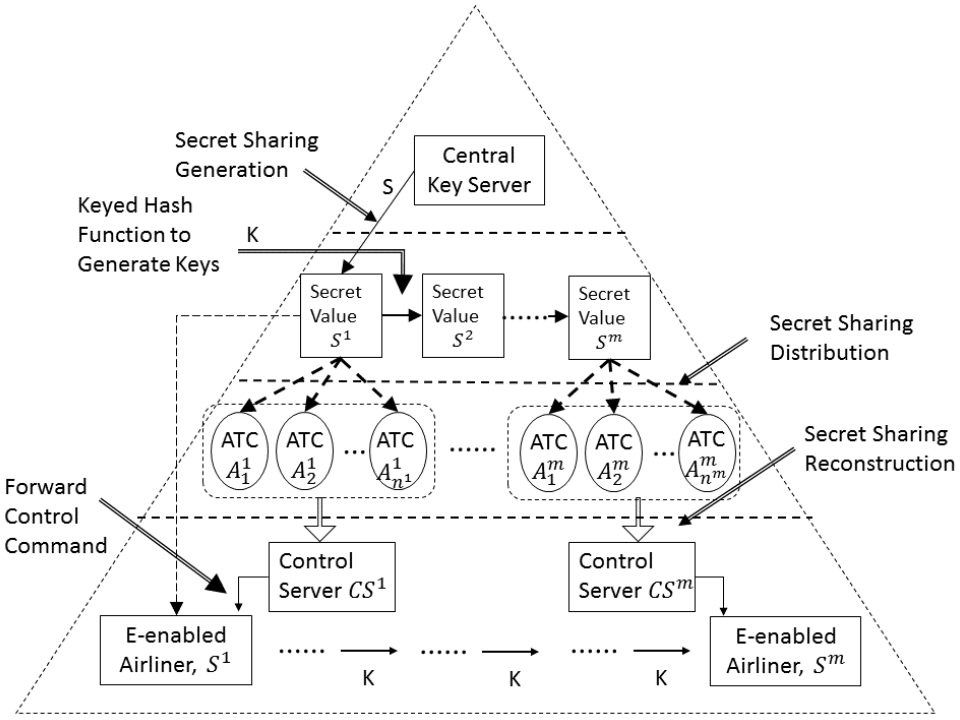

Fig. 3: Architecture of Secret Value Processing

F. Trust-based, Unequal, XOR-operation secret sharing

In this subsection, we will introduce our secret sharing scheme which includes three steps: *Setup*, *Distribution of secret sharing*, and *Trust evaluation engine and recovery of the secret value*. As compared to existing schemes, we focus on designing efficient, unequal, trust-based (t, n) threshold access control schemes in which $t' \leq x \leq t$ *where* n: the number of ATCs, t': the least threshold value, and t: the normal threshold value. Based on [51], it could satisfy the following requirements: (1) *single point of compromise resilience* (2) *efficient computation*, and (3) *secret recovery with less than* t *but larger than* t' *ATCs online*. Since only XOR-operations on binary strings, cyclic shift operations, addition, and floor of number operations are invoked, our solution, like [51], is efficient. Meanwhile, our (t, n) threshold secret sharing scheme are designed over general finite field $F = GF(q)$ *where* $q = 2$, all operations are processed over sequences of binary numbers and this makes our solution more efficient.

Setup of our secret sharing scheme: We assume that: (1) S is a secret value defined as $S = s_0 \cdots s_{\tau-1} \in F^\tau$ *where* S is a sequence of binary numbers and $\tau = |S| \geq n$. (2) p is a prime number with $gcd(p, q) = 1$ and $p \geq \tau + 1$. (3) the symbol $< a >_p$ denotes an integer b *where* $b \in \{0, \cdots, p-1\}$, a is an integer, and $b \equiv a(mod\ p)$. (4) t_{min}^j denotes the minimum number of ATCs online for country T^j *where* $t_{min}^j \geq t'$. t' should be predefined by country T^j to guarantee the aviation safety. (5) let $R(A_x^y)$ denote the trust value of an ATC who serves the country T^y. Meanwhile, $R(A_x^y)$ is calculated by our trust system described later in this subsection.

Secret Sharing Distribution: In this step, our procedure is described in the following sequence: (1) to generate a matrix $\mathbf{M}$ which will be used to distribute the secret sharing, (2) to define the maximum distance separable (MDS) linear code which is treated as Reed-Solomon code, and (3) to distribute the secret sharing.

Generation of Matrix $\mathbf{M}$: Our secret sharing scheme is defined as $\mathbf{M}$ over $F = GF(q)$ *where* $q = 2$ and $\mathbf{M}$ is a $(p-1) \times (n+1)$ matrix. Thus, $\mathbf{M}$ consists of $(p-1) \cdot (n+1)$ elements, namely, $c_{i,j}$ which is assigned in formula (1) and (2):

$$\mathbf{M} = \begin{cases} c_{i,0} = s_i, & \text{if } 0 \leq i \leq \tau - 1 \\ c_{i,0} = 0, & \text{if } \tau - 1 < i \leq p - 1 \end{cases} \tag{3}$$

Meanwhile, the $p \cdot (n-k)$ linear constraints are satisfied in $\mathbf{M}$:

$$\mathbf{M}_{[c_{i,j}]} = \sum_{j=0}^{n} c_{<h-jl>_p,j} = 0, \quad \textit{If } 0 \leq h \leq p-1 \textit{ and } 0 \leq l \leq n-t-1 \tag{4}$$

We will use a matrix $\mathbf{M}$ as our distributed secret. Briefly, the i^{th} column vector of matrix $\mathbf{M}$, namely, c_i, will be released to the i^{th} participating ATCs where $0 < i \leq n$.

Maximum Distance Separable (MDS): Let us describe how to convert a $[n, t, d]$ 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.

$$\begin{aligned} g(z) &= (z-1)(z-\alpha)\cdots(z-\alpha^{n-k-1}) \\ &= g_0 + g_1 z + \cdots + g_{n-k} z^{n-k} \end{aligned} \tag{5}$$

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 $c(z)$ can be used to encode the secret value later.

$$\begin{aligned} c(z) =& g(z)f(z) \\ =& g_0 f_0 + (g_0 f_1 + g_1 f_0) z + \\ & (g_0 f_2 + g_1 f_1 + g_2 f_0) z^2 + \cdots \end{aligned} \tag{6}$$

Secret Sharing Distribution: 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 sharings that will be distributed to each ATCs later. Let $N_p(x) = \sum_{i=0}^{(p-1)} x^i$ denote the polynomial and let R_p be the rings of $N_p(x)$. We also assume there is a root, α for $N_p(x)$ in ring R_p which satisfy $\alpha^p = 1$. Based on the denotation above, we define $r \times p$ matrix $\mathbf{H}$ where $r = p - t < p$

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(p-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(r-1)(p-1)} \end{pmatrix} \tag{7}$$

Let C be a linear code of length p over ring R_p with $\mathbf{H}$ as the parity-check matrix which is defined below:

$$C \triangleq \{c \in (R_p)^n | cH^T = 0\} \tag{8}$$

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 $\mathbf{H}$.

According to the proof in [7], if $\alpha \triangleq [1 \alpha \alpha^2 ... \alpha^{p-2}]$ is a basis of $R_p(q)$ over $F = GF(q)$, we can deduce that $C = \{c = \alpha\Gamma | \Gamma \in C(p-1, n, r)$ *where*

$$\mathbf{\Gamma} = \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & c_{1,2} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_{p-2,0} & c_{p-2,1} & c_{p-2,2} & \cdots & c_{p-2,n-1} \end{pmatrix} \tag{9}$$

Let $c = [c_0 c_1 ... c_{n-1}]$ be a codeword in C with each entry c_j working as an element in R_p. We can get that

$$c_j = c_j(\alpha) = \sum_{i=0}^{p-2} c_{i,j} \alpha^i \text{ where } c_{i,j} \in F, 0 \leq j \leq n-1 \tag{10}$$

Therefore, C will be identical to the code earn by regarding the columns of the array in $C(p-1, n, r)$ as elements in R_p.

Trust Evaluation Engine and Secret Value Distribution: In this step, we will describe our trust evaluation engine and explain how to assign the different number of secret shares to ATCs based on their trust values.

Based on [1], our direct trust scheme consists of three ways: (a) Familiarity-based trust value: When two ATCs work together, they recognize each others' performance, evaluate each others' behavior and finally rate each other. (b) Similarity-based trust value: Both ATCs have monitored the same pilot flying the same airliner at the same flight path. But they accomplished this at different times. They can assess each others' performance based on the recorded official report. (c) Condition-based trust value: Both ATCs have monitored the airliner under the similar extreme conditions such as severe weather (e.g. thunder, lightning), the similar terrain (e.g. mountain area), etc. Adapting PeerTrust model, our P-2-P integrated trust assessment scheme is calculated via formula (8):

$$\begin{aligned} R(A) = \mu \sum_{i=1}^{f_A} (S(A,i) \times CR(p(A,i)) \times TF(A,i)) \\ + \nu \times CF(A) \end{aligned} \tag{11}$$

where f_A denotes the number of flights an ATC A had monitored. $p(A,i)$ denotes that, at the i^{th} flight, P is another ATC who has worked together with A and $S(A,i)$ is the rating that P gives to A. $CR(x)$ denotes ATC x's credit score and $TF(A,i)$ is the trust value for flight i. $CF(A)$ is the trust value assigned to ATC A. Furthermore, $\mu + \nu = 1$ in which μ is the trust weight that others measure an ATC A and meanwhile ν the trust weight the system measure an ATC A.

Unlike traditional secret sharing scheme [47] in which each participant is assigned one secret shares, our idea is that we distribute the number of secret sharings to ATCs based on their trust values. We do not distribute secret sharing evenly. Thus, we may distribute more than one secret sharings i.e. α_j column vectors to one participating ATC, A_j if A_j's trust value is higher. Assume that we generate n secret sharings and there are t' ATCs *where* $n/2 < t' < t < n$. Our solution will assign each ATC one secret sharing and the rest $n - t'$ secret sharings will be assigned to the highest $n - t'$ participants.

Secret recovery: after collecting the secret sharing i.e. t numbers of c_js, we first calculate the syndrome values

$$\begin{aligned} \mathbf{s_l} = (y(H^T))_l = \sum_{i=0}^{(p-1)} e_i \alpha_i^l, \\ \textit{where } c = y, \ y = [y_0 y_1 \cdots y_{n-1}] \textit{ and } \alpha_i = \alpha^{j_i} \\ \textit{and } e_i = -c_{j_i} \textit{ and } 0 \leq i \leq p-1 \end{aligned} \tag{12}$$

Based on the syndrome values, the secret recovery scheme

should solve the linear system below:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{p-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{p-1}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_0^{p-1} & \alpha_1^{p-1} & \cdots & \alpha_{p-1}^{p-1} \end{bmatrix} \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{p-1} \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ \vdots \\ s_{p-1} \end{bmatrix} \tag{13}$$

Multiplying both side of the equation (11) with the inverse of $[\alpha_i^l]_{l,i=0}^{p-1}$, we can get the formula (12)

$$\begin{aligned} &\langle \prod_{s=0,s\neq i}^{p-1} (\alpha_i - \alpha_s) \rangle \times e_i = \sum_{l=0}^{p-1} G_{i,p-1-l} \times S_l \\ &\textit{where } 0 \leq i \leq p-1 \\ &\qquad G_{i,l} : l^{th} \textit{ symmetric function on } \{-\alpha_s\}_{0\leq s\leq p-1} \\ &\qquad G_{i,l} = G_{i,l}(\alpha) = \sum_{m=0}^{p-2} g_{m,i,l}\alpha^m \\ &\qquad S_l = S_l(\alpha) = \sum_{m=0}^{p-2} s_{m,l}\alpha^m, \\ &\qquad e_i = e_i(\alpha) = \sum_{m=0}^{p-2} e_{m,i}\alpha^m \end{aligned} \tag{14}$$

Therefore, we can extract e_i from formula (12) and finally recover the secret value S.

Assume that a set of ATCs $\{A_1, \cdots, A_{t_{min}}\}$ work together to recover the secret value. In formula (13), let $z(A_j)$ denote the number of secret sharings a participant A_j have been assigned. If $t \leq Y$, we say that the secret value could be recovered by the set of ATCs $\{A_1, \cdots, A_{t_{min}}\}$.

$$Y = \sum_{i=1}^{T_{min}} (z(A_i)) \tag{15}$$

Therefore, we could collect at least t secret sharings from t_{min} ATCs. Based on the decoding procedure aforementioned, we can recover the secret value. If we accomplish the secret sharing scheme on the finite field as $F = GF(2)$, the computational cost is $O(n(k-1)t)$ and the operations are solely bitwise XOR operations.

VI. Security Analysis and Performance Evaluation

In this section, a security analysis regarding our secret sharing scheme is provided at first. Then it follows the comprehensive analysis for the proposed solution. At last, we evaluate the performance, the assessment of which will be validated by concrete experimental results.

A. Security Discussion about Our Secret Sharing Scheme

In this subsection, first, we show that the proposed XOR-based secret sharing scheme can be viewed as Reed-Solomon type over the polynomial rings. This verifies that it is MDS. Second, we argue that MDS code could be converted to an ideal and linear (n, k) threshold sharing scheme.

Let R_p denote the rings of polynomials with the degree less than $p-1$. Meanwhile the ring also takes the multiplication module $M_p(x) = \sum_{i=0}^{(p-1)} x^i$. Based on the discussion in [8], we could show that there is a multiplicative inverse in R_p for each $r \times r$ sub-matrix of H (defined in equation (5)). Thus, the code C could be treated as the Reed-Solomon code over the ring R_p and then be considered as an MDS linear $[p, k, p-k+1]$ code.

According to [6], each $[n, k, d]$ MDS code could be transferred into a perfect and ideal (n, k) threshold secret sharing scheme (SSS). In detail, for a combinatorial definition of an ideal perfect SSS, we ensure that the code V of an ideal perfect (n, t)-threshold SSS is a q-ary code of length $n+1$, distance $d(V) \geq n-t+2$ and cardinality $|V| \geq q^t$ where $V = \{s \in S | P(s) > 0\}$ is the SSS code; $s = (s_0, s_1, ..., s_n) \in S = S_0 \times \cdots \times S_n$ is a sharing rule; let $S_0, S_1, \cdots, S_n$ be finite sets used by an SSS code; $q = |S_0|$; $P(s)$ is a probability distribution on S. Therefore, V is treated as an MDS code with $|V| = q^t$ and $d(V) = n-t+2$. We can also conclude that any MDS code satisfying aforementioned conditions could be converted into an ideal perfect (n, t)-threshold SSS.

In summary, our XOR-based secret sharing scheme is a non-empty MDS $[p, k, p-k+1]$ linear code over the ring R_p while it is treated as a $(p-1) \times p$ array code. At last, we conclude that our XOR-based (n, k) secret sharing scheme is not only complete but also private since any k participants could recover the secret value s and any subset of $k-1$ or less participants learn nothing about the secret value s.

B. Comprehensive Security Analysis

In this subsection, we discuss the security issue introduced by the threshold secret sharing, the chain of secret values, and the synchronization of secret values between the control server and the e-enabled airliner. Since the trust calculation is not closely related with the security issue, we will briefly analyzed it.

Trust-based, unequal, secret sharing: in this scheme, we assume that the secret share distribution and the secret share collection are undertaken in secret channel. Therefore, there should be no secret information leakage in this phases. Actually, as one of the most restricted network, the ATM system's secure communication technologies is mature and we could trust the security protection upon such kind of network communication settings. According 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 sharings could be collected if they all agree to take over the pilot's privilege. Therefore, the secret value s could be recovered. Thus, the security of trust-based, unequal secret sharing scheme can be presented.

Chain of secret values: The chain of secret values, $[S^1, S^2, ..., S^m]$ are calculated based on one way hash function with the following inputs, a randomly generated secret key K, a sequence of data X, and the master secret value MS. Since it is one way, there is no way that any country T^j can deduce T^i if $j > i$. Furthermore, the one way hash function utilizes the secret key K as the input, there is no way that any country T^i can deduce T^j if $j > i$. Therefore, it is secure.

Synchronization of secret values between control server and e-enabled airliner. When the airliner flies across a country T^j, the secret value S^j will be used for both the control server CS^j and the BHUAP devices. Therefore, they share the same secret value between each other and thus can encrypt and decrypt the control commands sent between them.

C. Computer Simulation

In this subsection, the proposed XOR-based secret sharing scheme is compared with Shamir's secret sharing scheme in terms of performance e.g. the execution time through implementing and executing simulation software on commercial PC. We utilize the SSSS-0.5 [42] as the simulation software. This free software package is developed upon UNIX/Linux platform. Its source codes are licensed under the GNU GPL v2. Both the share generation for a predefined secret and the secret reconstruction are implemented by using C++ programming language. The software links against the GNU *libgmp* multiprecision library (version 4.1.4). It also requires the */dev/random* entropy source in Linux to generate random values. Meanwhile, we implement the proposed XOR-based secret sharing scheme on Linux platform through invoking *Schifra Reed-Solomon ECC Library* [45] and integrating with other related open source cryptographic library in Linux. Our software prototype is developed by using C++ programming language. The compiler software and its version is GCC 3.3.1+. The experimental platform is based on a Virtual Machine (VM) hosted by a physical Dell PC, the configuration of which is listed as the following, *(CPU: Intel (R) Core (TM) i7-4770 @ 3.40GHZ and Memory: 8192MB)*. The VM software and its version is Oracle VM VirtualBox version 5.0.12. The specific configuration of the VM is listed as the following, *(Base Memory: 1024 MB; Video Memory: 12 MB; SATA Storage: 18.00 GB. The loaded OS is Ubuntu 14.04)*.

In our experiments, the size of the secret is 1KB. We have tested 9 pairs, i.e. *(k,n)* = {*(3,4), (5,11), (7,8), (5,11), (10,14), (12,15), (14,16), (15,18), (17,19), (13,25)*} *where* k is the threshold values and n the total number of spitted sharing. Both the secret share distribution component and the secret value recovery component of the proposed SSS scheme and Shamir's SSS scheme have been executed in our experiments. The results of the proposed scheme are depicted in Fig. 4 and that of Shamir's scheme in Fig. 5. On both figures, the x-label is the (threshold value, total number of the sharing) pair and the y-label the execution time. As demonstrated in Fig. 4, the execution time of the secret distribution component and of the secret recovery component for proposed SSS scheme is ranging

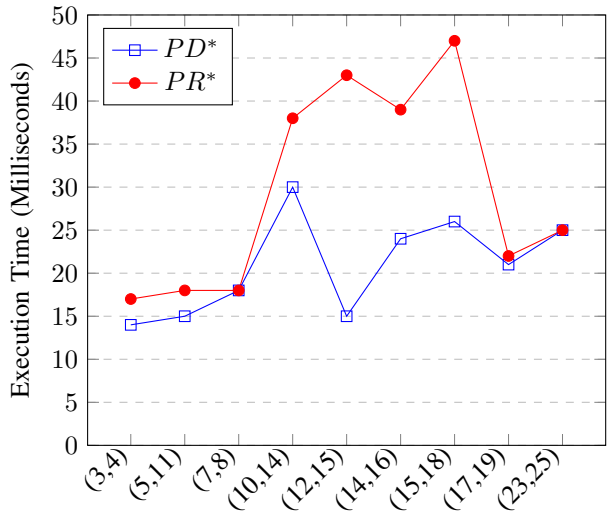

Fig. 4: Performance of Proposed SSS Scheme
PD* - Proposed Secret Distribution; **PR*** - Proposed Secret Recovery

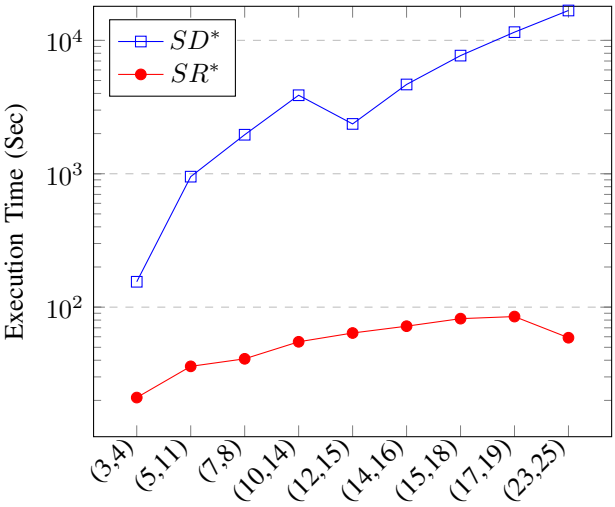

Fig. 5: Performance of Shamir's SSS Scheme
SD* - Shamir's Secret Distribution; **SR*** - Shamir's Secret Recovery

from 14ms to 30ms and from 17ms to 47ms, respectively. Fig.5 shows that the execution times of the secret distribution component and of the secret recovery component for Shamir's SSS scheme is ranging from 155 seconds to 16745 seconds, and from 21 seconds to 85 seconds, respectively. Based on the experimental results, we conclude that the proposed scheme is significantly efficient than Shamir's SSS scheme regarding not only the secret distribution component but also the secret recovery component.

D. Performance Evaluation

In this subsection, we will evaluate the cost of the proposed solution in terms of computational and communication over-

head as well the cost to adopt our system for ATM systems. In detail, regarding the we will carefully evaluate different criteria in terms of two fundamental components: (1) the trust-based, unequal, secret sharing scheme which relies on bitwise XOR operations, and (2) Chain of secret values.

Computational Cost — Bitwise XOR-operation for our Secret Sharing Scheme: As we analyzed in subsection V(F), if we let $q = 2$, our operations are executed over binary sequence. Thus, our secret sharing scheme only executes the bitwise XOR operations which are computational efficient. If we accomplish the secret sharing scheme on the finite field as $F = GF(2)$ and let $n_p = n$, the computational cost is $O(n(k-1)|s|)$ (*where* s is a secret value string) and the operations are solely bitwise XOR operations. In detail, our bitwise XOR-based secret sharing scheme consists of the following two phases:

(1) Share generation component: In this phase, the amount of computational overhead depends on the number of bitwise XOR operations. We can evaluate it by counting the number of "1"s in a column of H. Based on the nature of the matrix, the upper bound cannot exceed k. Thus, our assessment is that, to compute the secret shares, the maximum number of bitwise XOR operations is $O(n(k-1)(p-1)d = n(k-1)|s|) = O(n(k-1)t)$.

(2) Secret value recovery component: The number of Gaussian elimination or some similar operations over GF(2) is H while achieving the goal of the secret recovery. On the other hand, the computational cost to process modulo operations on indexes is similar as that of deploying fixed parity check matrix. Since the computational cost of the latter is trivial, modulo operations are negligible in our performance evaluation. Consequently, the overall computational cost for our bitwise XOR secret value recovery scheme is $O(((kn_p)\cdot\log_2 t)+k^3n_p^3)$ (*where* $t = |s|$ and $n_p = n$) which is treated as the upper bound. As compared to the computational cost of secret generation scheme which demands $O(n(k-1)t)$, the secret value recovery component requires more number of bitwise XOR operations. Our experimental results depicted in Fig. 4 support this performance evaluation.

Computational Cost — Arithmetic Operation for Shamir's Secret Sharing Scheme: Share generation component vs. Secret value recovery component of Shamir's scheme: according to [47], the share generation component in Shamir's scheme demands $O(kn)$ arithmetic operations and the secret value recovery component requires $O(k\log^2 n)$ ones. Therefore, the processing time for the share generation operation is longer than that of share recovery operation. Our experimental results depicted in Fig. 5 support this performance evaluation.

Computational Cost — Chain of Secret Values: The generation of multi-secret value demands one random number generation and $l-1$ times DES encryption operations. The execution time of them are trivial upon current commercial PCs which normally are deployed with powerful CPUs.

Communication Overhead: The communication overhead includes (1) the distribution of l secret value to the airliner, (2) the distribution of secret sharing to each ATC (nl numbers of sharings should be released in total), and (3) the collection of tl numbers of secret sharings from all ATCs.

Expense to adopt the proposed solution: For this proposed solution, the existing air traffic control system e.g. the ground devices, the control system on the airliners and the network communication system in between is the most expensive asset, the legitimacy of various tracks of history for all pilots are the most important data set. Since primary ATM systems are already established and the pilot performance evaluation are already been accomplished, the proposed solution do not demand any further costs in terms of hardware. The implemented software prototype is mainly based on open source library. Consequently, the adoption of the proposed solution is feasible for ATM system.

In summary, our threshold-based access control solution is solely based on XOR operations which demand trivial computational costs and execute in a very short time. This has already been justified by the experimental results in [20]. Thus, we believe that the performance results are predicable and they satisfy the requirements of the aviation system.

VII. Conclusion and Future Works

Airliner incidents indicate that when pilots are manipulated by hijackers or pilots intend to commit suicide, the airliner is dangerous and the target on ground can be threaten. Though being a safer solution, the BHUAP is yet deployed in the airliner due to pressing challenges such as the single point of compromise of ATCs especially when the airliner flies multiple countries. In this paper, we propose a new access control framework to mitigate the corresponding risk for the airliner flying across multi-countries. It is efficient and it assures that each country could have its own secret value in the air traffic management system. The proposed XOR-based secret sharing scheme has been developed and implemented. Its experimental results demonstrate its high performance over existing secret sharing schemes. The performance evaluation and security analysis further show that our novel framework is feasible, secure, and efficient.

Our future work will emphasize on two open questions. First, based on further optimization analysis and the accumulation of future field test results, we will predict and define the least threshold value and normal threshold value which play an important role in this system. Second, regarding the fixed value of n in the n, k threshold method, false alarms for different values of the threshold are important while achieving applications such as the access control mechanism. Therefore, how to define, recognize and trigger false alarms upon varied context and different scenarios will be studied.

References

[1] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, pages 9–pp. IEEE, 2000.

[2] 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.

[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] G. R. Blakley and G. A. Kabatianski. Ideal perfect threshold schemes and mds codes. In *Proceedings., 1995 IEEE International Symposium on Information Theory*, pages 488–488. IEEE, 1995.

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

[9] A. Brauchli and D. Li. A solution based analysis of attack vectors on smart home systems. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, pages 1–6. IEEE, 2015.

[10] 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.

[11] 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.

[12] 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.

[13] R. Cramer and S. Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In *Crypto*, pages 31–37, 2002.

[14] Y. G. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. In *SIAM journal on Discrete Mathematics*, pages 667–679, 1994.

[15] E. Goode. Suicide by plane crash is rare but not without precedent. *[Online]: http://www.nytimes.com/2015/03/27/world/europe/few-precedents-are-seen-as-germanwings.html*, March 2015.

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

[17] K. F. J. Kurihara, S. Kiyomoto and T. Tanaka. A fast (3, n)-threshold secret sharing scheme using exclusive-or operations. In *IEICE Trans. Fundamentals*, pages 127–138. IEICE, 2008.

[18] R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu. Practical secret key agreement for full-duplex near field communications. *IEEE Transactions on Mobile Computing*, 15(4):938–51, April 2016.

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

[20] K. S. F. K. Kurihara, J. and T. Tanaka. A new (k, n)-threshold secret sharing scheme and its extension. In *In International Conference on Information Security*, pages 455–470. Springer Berlin Heidelberg, 2008.

[21] D. Li. Mitigate airliners' risk via intervening critical controls by leveraging authenticated secret sharing. In *Aerospace Conference, 2016 IEEE*, pages 1–9. IEEE, 2016.

[22] D. Li. Pick a right puppy from a litter, toward a secure controller framework in physical, human and cyber triad. In *Information Technology, Networking, Electronic and Automation Control Conference, IEEE*, pages 98–102. IEEE, 2016.

[23] D. Li, Z. Aung, J. Williams, and A. Sanchez. P3: privacy preservation protocol for automatic appliance control application in smart grid. *Internet of Things Journal, IEEE*, 1(5):414–429, 2014.

[24] D. Li and R. Zhang. A framework to mitigate airliner risk in air traffic management. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2016.

[25] T. Li, R. Zhang, and Y. Zhang. Priexpress: Privacy-preserving express delivery with fine-grained attribute-based access control. In *Communications and Network Security (CNS), 2016 IEEE Conference on*, pages 333–341. IEEE, 2016.

[26] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao. A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems. *IEEE Transactions on Vehicular Technology*, 66(3):2551–2566, March 2017.

[27] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, PP(99):1–1, 2017.

[28] C. Lv, X. Jia, L. Tian, J. Jing, and M. Sun. Efficient ideal threshold secret sharing schemes based on exclusive-or operations. In *In Network and System Security (NSS), 2010 4th International Conference on*, pages 136–143. IEEE, 2010.

[29] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. Elsevier, 1977.

[30] S. Marsden and R. Massey. Why can't airlines seize control of doomed jets from the ground? the technology exists but pilots and companies refuse to use it. *[Online]: http://www.dailymail.co.uk/news/article-3013858/Why-t-airlines-seize-control-doomed-jets-ground-technology-exists-pilots-companies-refuse-use-it.html*, March 2015.

[31] Y. F. M. T. N. Hosaka, K. Tochikubo and T. Kato. (2, n)-threshold secret sharing systems based on binary matrices (in japanese). In *Proc. SCIS2007*, pages 2D1–4, 2007.

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

[33] A. S. Network. Investigators: Lam embraer 190 accident likely intentionally caused by pilot. *[Online]: http://news.aviation-safety.net/2013/12/22/investigators-lam-embraer-190-accident/*, 2009.

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

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

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

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

[38] U. D. of State International Information Programs. U.s. aviation agency sets standards for cockpit security. *[Online]: http://cryptome.org/faa-cocksec.html*, 2002.

[39] 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.

[40] 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.

[41] R. Pocklington and B. Burrows. Missing malaysia airlines flight: 13 conspiracy theories surrounding disappearance of mh370. *[Online]: http://www.mirror.co.uk/news/world-news/missing-malaysia-airlines-flight-13-3412956*, April 2014.

[42] B. Poettering. Shamir's secret sharing scheme. *[Online]:http://point-at-infinity.org/ssss/.*, 2006.

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

[44] 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.

[45] Schifra. Reed solomon codec performance. *[Online]:http://schifra.com/fqa.html*, 2006.

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

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

[48] 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.

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

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

[51] 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.
[52] C. A. Wargo and C. Dhas. Security considerations for the e-enabled aircraft. In *IEEE Aerospace Conference*, 2003.
[53] W. Website. Ground proximity warning system. *[Online]: https://en.wikipedia.org/wiki/Ground-proximity-warning-system*, 1996.
[54] W. Website. Boeing honeywell uninterruptible autopilot. *[Online]: https://en.wikipedia.org/wiki/Boeing-Honeywell-Uninterruptible-Autopilot*, 2006.
[55] W. Website. Unmanned aerial vehicle. *[Online]: http://en.wikipedia.org/wiki/Unmanned-aerial-vehicle*, 2014.
[56] W. Website. Autopilot. *[Online]: https://en.wikipedia.org/wiki/Autopilot*, 2015.
[57] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema. Toward integrating distributed energy resources and storage devices in smart grid. *IEEE Internet of Things Journal*, 4(1):192–204, Feb 2017.
[58] K. Yang, X. Jia, K. Ren, B. Zhang, and X. R. Dac-macs: effective data access control for multiauthority cloud storage systems. In *IEEE Transactions on Information Forensics and Security*, pages 1790–1801. IEEE, 2013.
[59] 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.
[60] W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie. Ultra-dense networks: Survey of state of the art and future directions. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–10, Aug 2016.
[61] 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.
[62] 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.