DPP: Dual Path PKI for Secure Aircraft Data Communication

Alexander K. Buchholz

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Science

In

Computer Science and Applications

Wenjing Lou, Chair

Ing-Ray Chen

Charles T. Clancy

April 29th, 2013

Falls Church, Virginia

Keywords: Air Traffic Control, ADS-B, PKI, ECC, Certificate Revocation

Abstract

DPP: Dual Path PKI for Secure Aircraft Data Communication

Alexander K. Buchholz

Through application of modern technology, aviation systems are becoming more automated and are relying less on antiquated air traffic control (ATC) voice systems. Aircraft are now able to wirelessly broadcast and receive identity and location information using transponder technology. This helps reduce controller workload and allows the aircraft to take more responsibility for maintaining safe separation. However, these systems lack source authentication methods or the ability to check the integrity of message content. This opens the door for hackers to potentially create fraudulent messages or manipulate message content.

This thesis presents a solution to handling many of the potential security issues in aircraft data communication. This is accomplished through the implementation of a Dual Path PKI (DPP) design which includes a novel approach to handling certificate revocation through session certificates. DPP defines two authentication protocols, one between aircraft and another between aircraft and ATC, to achieve source authentication. Digital signature technology is utilized to achieve message content and source integrity as well as enable bootstrapping DPP into current ATC systems. DPP employs cutting-edge elliptic curve cryptography (ECC) algorithms to increase performance and reduce overhead.

It is found that the DPP design successfully mitigates several of the cyber security concerns in aircraft and ATC data communications. An implementation of the design shows that anticipated ATC systems can accommodate the additional processing power and bandwidth required by DPP to successfully achieve system integrity and security.

Acknowledgements

I would like to express the deepest appreciation to my thesis advisor Wenjing Lou who was abundantly helpful through all her support, guidance, and sharing her extensive knowledge during this process. Without her encouragement and advice the success of this thesis would not have been possible. I would like to thank my committee members, Dr. Ing-Ray Chen and Dr. Charles Clancy for agreeing to be on my board.

I am indebted to many of my colleagues whose support I will not soon forget. I'd like to specifically thank Doug Vandermade for many hours of intense discussion and debate arguing the solutions to many difficult problems in the world. His leadership and mentoring is greatly appreciated and will have positive and lasting effects on me for the rest of my life. I'd also like to thank Doug Havens and Brock Lascara for their friendship and support and helping me rubber-ducky my way through many of the difficult concepts discussed in this paper. I would also like to thank Brennan Haltli, Quang Nguyen, Rob Strain and several others at The MITRE Corporation for their help and support as well.

With a full heart I thank my beautiful wife, Melissa Buchholz, amazingly supportive parents Teresa and Harald Buchholz, and my many encouraging friends for all their love, help, and understanding during this process. This thesis would have remained a dream had it not been for them. Words cannot describe the appreciation and gratitude I have towards their huge contributions and positive attitudes. It truly takes a village and I am lucky to be a part of a great one.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
ADS-B	Automatic Dependent Surveillance-Broadcast
AIAA	American Institute of Aeronautics and Astronautics
ANSI	American National Standards Institute
ARTCC	Air Route Traffic Control Centers
ARTS	Automated Radar Terminal System
ATC	Air Traffic Control
ATRCRBS	Air Traffic Control Radar Beacon System
CA	Certificate Authority
CPDLC	Cockpit to Controller Data Link Communications
CRL	Certification Revocation List
CSS	Critical Services Specification
DH	Diffie-Hellman
DOT	Department of Transportation
DPP	Dual Path PKI
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EFB	Electronic Flight Bag
ERAM	En Route Automation Modernization
ES	Extended Squitter
FAA	Federal Aviation Administration
FTI	Federal Telecommunications Infrastructure
ICAO	International Civil Aviation Organization
IEEE	Electrical and Electronics Engineers
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
ISO	International Organization for Standardization
MIPS	Million Instructions Per Second
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NGIP	NextGen implementation plan
NIST	National Institute of Standards and Technology
OpSpec	Operations Specification
PKI	Public Key Infrastructure
SBSS	Surveillance Broadcast Service System
STARS	Standard Terminal Automation Replacement System

TRACON	Terminal Radar Approach Control Centers
UAT	Universal Access Transceiver
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad Hoc Networks
WAM	Wide Area Multilateration

Chapter 1
Introduction

1.1 Motivation

Secure communication is of growing concern in an increasingly connected world. Essential data that is communicated in the open is vulnerable to variety of attacks which could jeopardize system integrity. This is an issue in many domains due to the increasing applications of the internet and wireless data communications. There is concern that without continued research into robust cyber security methods critical systems that the populous rely on could be susceptible to attack. This is of special interest in areas where the reliance on data confidence and source identification is of utmost importance to the safety of human lives. One such example is in the domain of aviation where data communication and robust identification methods between aircraft and air traffic control (ATC) is relied upon to preserve safety.

For years aircraft and ATC have passed important information using radio and other low tech methods [1] . However, with the continued growth of airport traffic more efficient data communication methods are beginning to be implemented [1]. These new technologies allow aircraft and ATC to communicate pertinent information real-time using data link technologies while reducing overall pilot and controller workloads [1] . This revolution in data dissemination is a huge breakthrough in modernizing the aging ATC communications system and could drastically improve many critical ATC functions. However, it presents a number of security and safety concerns. This paper discusses those concerns and presents a novel way of overcoming many of them.

1.2 Thesis Contribution

There is growing speculation that inclusion of modern cyber security methods might have properties advantageous to the security and integrity of ATC data communication systems [2] [3] [4] [5]. However, the design through which these methods are implemented is tantamount to the security of the resulting system. Without the use of proper techniques unforeseen outcomes such as trap doors and unintended security weaknesses can arise [6]. Meticulous research in the domain of aviation data communication and a strong understanding of cyber security primitives must be thoroughly presented before a robust security design can be formulated.

This thesis is among the first to address the issues of insecure aircraft-to-aircraft and aircraft-to-ATC data communications. It includes a discussion of the state of the art in aircraft identification and data validation methods and specifies potential security vulnerabilities. A formalized list of requirements to fill this gap is suggested. Furthermore, this thesis proposes a public key infrastructure (PKI) to work within the existing ATC system and provide key management for aircraft and ATC. A novel approach to certificate revocation is suggested through the implementation of session certificates. A suite of mutual authentication protocols are described along with suggested encryption algorithms. Lastly, a feasibility study is performed to evaluate the potential performance of the system.

1.3 Thesis Outline

The contents of each chapter are described as follows. Chapter 2 lays out all background information regarding ATC's aircraft identification and monitoring practices. Then there is a discussion on where the gap in knowledge lies. It also contains information regarding the cyber security primitives that will be employed to fill that gap in knowledge. Chapter 3 explicitly states the problem definition along with requirements for the solution. There is also an attack model which lists potential attacks to the system. Chapter 4 describes the design along with all protocols and procedures utilized to

accomplish the goals described in Chapter 3. Chapter 5 is an analysis of the solution which states explicitly how each requirement it met and how each attack is mitigated. Chapter 6 is an evaluation of the solution and discussed how it should perform when applied. Chapter 7 is the conclusion where all results are abstracted and briefly discussed.

Chapter 2
Background

This section describes the fundamentals of ATC aircraft identification and monitoring practices as they evolved starting from the inception of aviation. Then the effects of modern technologies are discussed and how upgrades to system security are warranted. In addition, cyber security primitives such as public key encryption along with PKI are defined as they relate to the solution proposed in this paper. Then the gap in knowledge is stated. The following section has a literary review on related works which includes some references to similar issues in other domains and how they were overcome.

2.1 Development of ATC's Aircraft Identification and Monitoring

Accurately determining an aircraft's identity and location has been and will continue to be a difficult task for the aviation community. These truths are important for security, safety, and efficiency of the ATC system. Most notably, knowing an aircraft's location is important to prevent midair collisions. In most situations when the weather is clear pilots are told by ATC where other aircraft are and they can confirm via line of sight [1]. However, in times of low visibility when aircraft cannot see and avoid aircraft around them, known as instrument meteorological conditions (IMC), law requires pilots to use instrument flight rules (IFR) to navigate [1]. In short, aircraft rely solely on ATC to communicate who and where other aircraft are [1]. This requires ATC to have robust methods for accurately determining who and where an aircraft is.

2.1.1 Early Monitoring Systems

In ATC's early years rudimentary techniques were used to communicate with aircraft but little was done to ensure their identity. Controllers used a manual technique of moving "shrimp-boats" on a map, each of which represented individual aircraft [1] . The controllers would receive updates from aircraft over radio communication and would

then update the shrimp-boat location while also relaying necessary information to other aircraft in the area. After the implementation of radar to ATC monitoring systems in the 1940's controllers could more accurately and efficiently determine the real-time positioning of aircraft [1]. Controllers used radar to determine aircraft location and radio to communicate this information to each pilot flying IFR. This system worked reasonably well for many years [1]. As air travel became more popular towards the middle of the 20th century overall traffic volume increased in the national airspace system (NAS). With the increase in traffic came a dramatic increase in controller workload and the tedious task of constantly maintaining the connection between the identity and location of each aircraft became more of a burden. As computer technology advanced the next step of real time automation systems to handle this controller task became apparent.

2.1.2 Evolution of Automated Radar Terminal System

The evolution of how ATC tracks an aircraft's identity and location relied on two technologies: 1) the development of radio frequency identification using transponders and 2) electronically filed flight plans [1]. The former, known as the secondary radar system, uses pulses and modes of radio signals to send data between aircraft and ATC [1]. Each aircraft that operates in the NAS has a transponder code which is assigned when it is built. Widely considered as the most significant development in ATC technology, the Air Traffic Control Radar Beacon System (ATRCRBS) uses transponder codes to determine the identity of an aircraft through a radio-based interrogation and response mechanism [1]. This system was first introduced in 1956 and eventually spread to ATC centers all over the NAS after a few years. The transponder codes are cross referenced with flight plan information (#2 above) to give the controller all the flight specific information for the aircraft such as flight number and registration information. These flight plans are filed prior to takeoff and are sent to all controllers who require information from them. They also give the controller a notion of when an aircraft should be where and is used as a double check to radar sources.

The cross referencing of various, possibly inaccurate sources creates a sort of information assurance synergy that is now the backbone of ATC's modernized approach

to aircraft location and identity. One successful implementation of this system is known as the Automated Radar Terminal System (ARTS) which is used across the country at en route control centers known as Air Route Traffic Control Centers (ARTCCs) and terminal control centers known as Terminal Radar Approach Control Centers (TRACONs) [1]. The next section discusses how the ARTS system evolved to include modern technologies and more efficient automation techniques.

2.2 State of the Art Aircraft Identification and Monitoring

As location and communication technologies advanced a number of new systems to handle many of the tedious tasks required by aircraft and ATC were developed. These technologies included such things as the development of the global positioning system (GPS), robust and secure data communications infrastructure, and efficient real-time data fusing algorithms. As a result the Federal Aviation Administration (FAA) and industry created a number of upgraded systems to handle the identification and monitoring of aircraft, some of which will be implemented through the Next Generation Air Transportation System (NextGen). The goal of NextGen is to enhance safety and increase efficiency in the NAS. This system is set to be deployed in segments over the next several years [7]. The NextGen implementation plan (NGIP) details how the system is planned to be implemented [8]. The NGIP will be used as a reference later during the performance analysis.

Some of the systems the FAA and other government agencies are implementing include Automatic Dependent Surveillance-Broadcast (ADS-B), Federal Telecommunications Infrastructure (FTI), and two extensions of the ARTS system: 1) Standard Terminal Automation Replacement System (STARS) and 2) En Route Automation Modernization (ERAM). Each one of these systems is discussed below along with why they are important to the modernization of aircraft identification and monitoring. At the end of this section a brief overview of the system is discussed which includes exactly where the gap in knowledge lies.

2.2.1 ADS-B

GPS revolutionized aircraft position monitoring. No longer does an aircraft need to rely solely on ATC or other antiquated systems to determine its location. Aircraft use GPS to determine accurate position and velocity information which is derived through an on-board flight management system [9]. However, GPS only helps the aircraft know its own location. Without a standard high update data communication system ATC and other nearby aircraft still require the use of passive systems to determine other aircraft identity and location. This led to the development of ADS-B and an FAA mandate that requires all aircraft be equipped by 2020 [8]. This system broadcasts information regarding the aircraft's identity and current position using a similar transponder technology as the ARTS system [10]. ADS-B utilizes two different transponder technologies: 1) ADS-B 1090 Extended Squitter (ES) and 2) Universal Access Transceiver (UAT) [9]. Similar in nature, both transponder technologies continuously broadcast identity, target state (position, velocity, time), and other status information [9]. However, aircraft can only send and receive messages from other aircraft equipped with the same transponder technology [11]. This requires a network of towers to relay the messages. Figure 2-1 below illustrates ADS-B service data flows between similarly equipped aircraft and ATC.

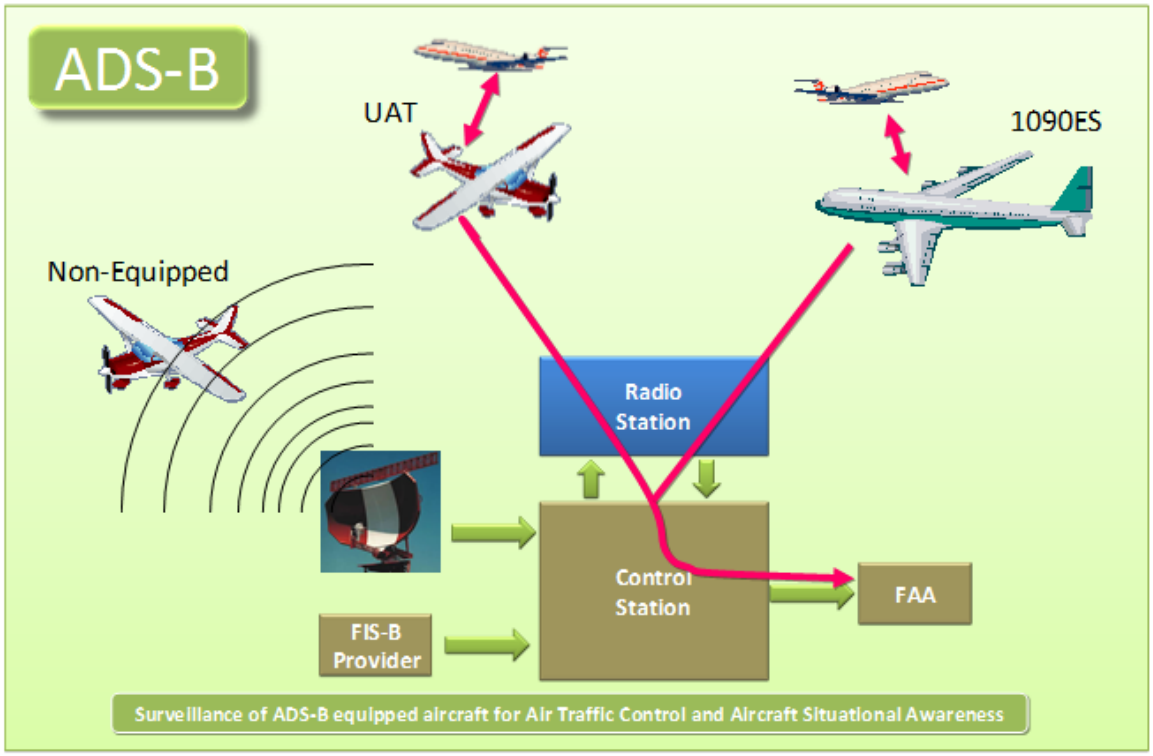

Figure 2-1. ADS-B Service Data Flows **[9]**

ADS-B is only one component of a much larger system known as the Surveillance Broadcast Service System (SBSS) [9]. This system handles weather, traffic, aircraft identification and location, and other message types and disseminates this information to those who need it [9] [11]. The SBSS includes a network of towers which relay the ADS-B messages received to other aircraft in the area as well as ATC [11]. This is the mechanism through which ATC receives ADS-B messages from aircraft.

ADS-B allows for direct information sharing between aircraft which could completely revolutionize the way aircraft identify and separate themselves from other aircraft. As noted in section 2.1, aircraft flying IFR are required by law to consult with ATC to separate themselves from aircraft around them. ADS-B has many potential applications; one of which allows aircraft to handle maintaining separation by receiving location information directly from the aircraft around them instead of through ATC [1]. Considering the update rate, 1Hz, and accuracy, GPS, of the location information in the ADS-B messages, aircraft could drastically reduce separation standards along with significantly reduce the workload for controllers [10]. Note, however, that these

messages are broadcasted in their raw form and are susceptible to manipulation or forgery.

Now that aircraft can talk directly to each other there needs to be an equivalent system that allows each entity within the ATC system to communicate to each other. This includes all ATC centers, the FAA, as well as aircraft on the ground. The next section discusses the FTI system and how it relates to this paper.

2.2.2 FTI

In the early days of ATC, centers were required to communicate with each other through phone calls [1]. When an aircraft became a new center's responsibility the old center literally picked up the phone and called the new center to alert them to the aircraft's arrival [1]. This system cannot be sustained with the continued growth in aircraft traffic. The development of the internet allowed for the digital interconnections between ATC centers and the FAA. However, a level of security was required to make these connections secure. The design of the FTI accounts for this and develops secure ground connections between entities necessary to the functions of FAA and ATC [12] . Figure 2-2 illustrates the FTI system and how ATC centers and the FAA are connected via data link [13].

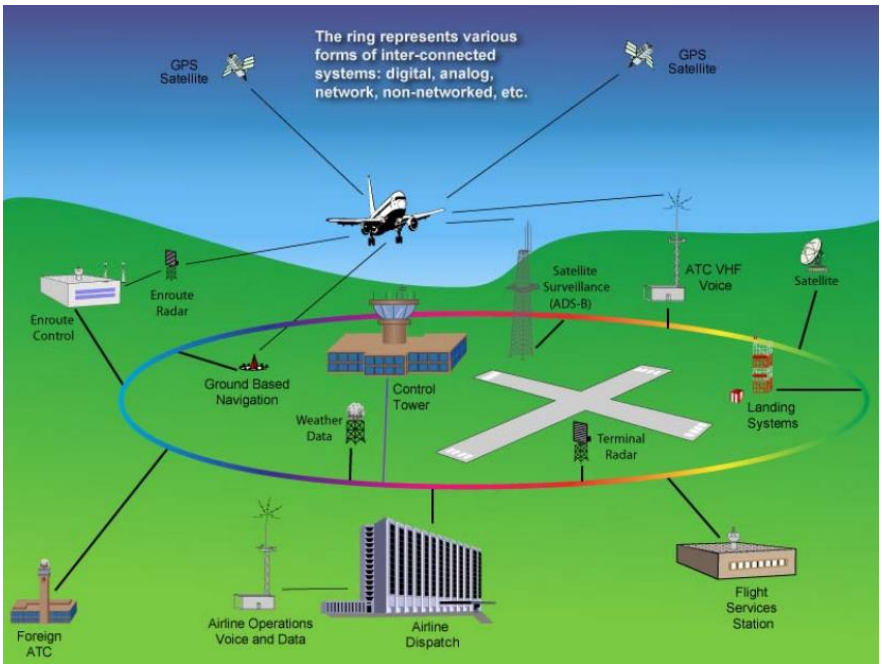

Figure 2-2. A layout of the FTI system [13]. Note the connection between each control tower (TRACON), the flight services station, the en route control center (ARTCC), and the SBSS (ADS-B). FTI services ensure secure communications between all ground based systems. Note that this does not include aircraft-to-aircraft and ATC-to-aircraft communications

An important utilization of the FTI system is the dissemination of electronic flight plans. Flight plans include information regarding the route of an aircraft which lists each ARTCC and TRACON that the aircraft will fly through. When uploaded at the ATC center that the aircraft is departing from, that center securely sends out the flight plan to all centers that may require it. Assuming FTI's robust security it can also be used as infrastructure to handle information necessary to the implementation of cyber security methods. This is discussed later in the paper.

The development of both the FTI and SBSS allowed for significant upgrades to the ARTS system. With ADS-B the ARTS system can include GPS data and FTI will allow for collection and implementation of digital flight plans. The next section discusses these updates through the STARS and ERAM systems.

2.2.3 STARS and ERAM

Standard radar and beacon systems are relatively accurate and are helpful in the automation of aircraft identification and monitoring at ATC centers. However, through

the development the SBSS ATC now has access to ADS-B messages and the GPS location information inside them. To increase the accuracy of systems which utilize ATCRBS, ADS-B location information is fused with radar surveillance information. This is done in systems like STARS and ERAM which are utilized at TRACONs and ARTCCs, respectively [14] [15]. Both systems receive ADS-B target position data through SBSS and fuse it with radar signals from the ATCRBS. This is accomplished through a multilateration technology called Wide Area Multilateration (WAM) [16]. Once an aircraft's location is confidently determined, known flight plan information is included to add other valuable information and presents everything to the controller. This data fusing is illustrated in Figure 2-3 below.

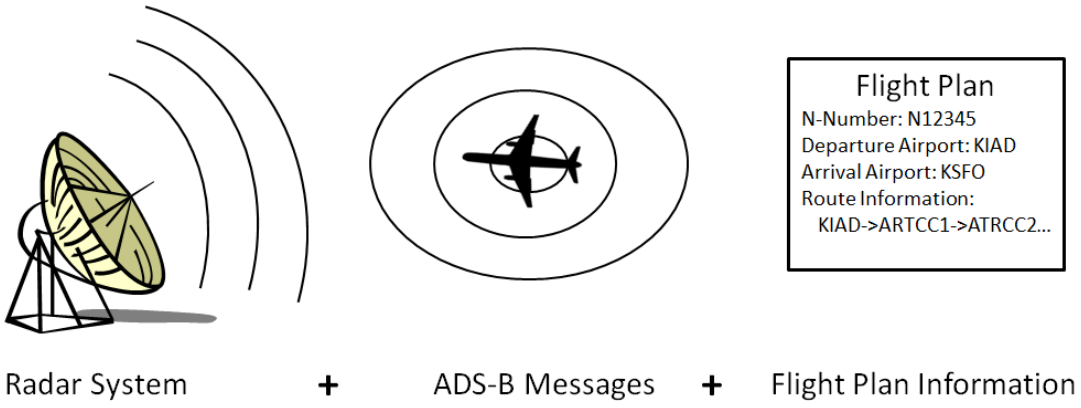

Figure 2-3. Data fusing method utilized by ERAM and STARS

In order for these systems to rely more heavily on ADS-B messages ATC needs a way to ensure that each message is sent from a reliable source and that the content has not been manipulated. These issues reveal a potential security risk with the system which is discussed in greater detail in the next section.

2.2.4 Gap in Knowledge

These systems are relatively secure when a controller is using raw radar information along with known and trusted flight plan data. However, with the inclusion of a data source that comes directly from the aircraft there are a few security risks that are

addressed through ADS-B "Independent Validation" as specified in the Department of Transportation (DOT) critical services specification (CSS) document [11]. The validation is done through 1) comparison to radar, 2) comparing a one way "passive range" with range to target indicated by ADS-B, and 3) use of time difference of arrival techniques [11]. These methods, although robust in physical nature, do not present a way to authenticate or validate specific ADS-B messages. In certain scenarios, like when aircraft are much closer during parallel arrival and departure, there might not be enough time for this validation step. Also, it is important to note that a simple check of the ADS-B message contents would reveal the transponder code and ATC could authenticate that way. However, along with other threats, messages can be spoofed using someone else's transponder code [17] [18]. Other potential risks to the system are described in Chapter 3.

In summary, the main issue with raw aircraft-to-aircraft and aircraft-to-ATC data communication is authentication and integrity protection. Without being absolutely sure who the message came from along with assurance that the messages have not been manipulated the system cannot rely solely on ADS-B. Therefore ADS-B cannot be used to supplement current procedure design and reduce separation minimums without the risk of spoofing and content manipulation. Standard cyber security primitives such as public/private key encryption and PKI could be employed to handle many of the issues noted above. However, this domain has some requirements that an individual PKI might not be able to handle. Not only do aircraft and ATC need to authenticate and integrity check messages, specific aircraft in the sky might need more to be absolutely sure of where another aircraft is. This will require authentication of an aircraft's identity both from the FAA and, more importantly, the local ATC center. This paper discusses a solution which includes a robust PKI along with effective and efficient public key protocols for message authentication and integrity protection. These cyber security primitives are discussed in the following section.

2.3 Cyber Security Primitives

In the following section basic cyber security primitives are explained. These include public key cryptography as well as PKI design as they relate to the issues noted in aircraft and ATC communications discussed in the previous section.

2.3.1 Public Key Cryptography

Public key cryptography, sometimes known as asymmetric cryptography, utilizes modern number theory to create two keys for an individual, one public and one private, which work together to accomplish a number of security objectives. The special nature of public key cryptography allows one to encrypt a message with one key, let's say the private key, and the only way to decrypt is with the other, the public key [6] [19]. In order for the system to work the private key must be kept secret by the owner. This is because the private key is used to authenticate a user; if someone receives a message encrypted with a specific private key and they have the associated public key they can be sure that the message came from the entity who signed it with their private key [6] [19].

For ease of explanation and interpretation of public and private key encryption, curly braces "{x}" denote public key encryption and brackets "[x]" denote private key encryption. Typically braces and brackets are followed by a subscript letter or code. This subscript indicates who owns the public or private key used during the encryption. [6] [19].

In the context of this paper, each aircraft and ATC center are required to have private keys and everyone else, all other aircraft and ATC centers, need to gain access to their public key. This would allow each entity to encrypt messages with their private keys and everyone else could decrypt with the associated public key.

2.3.2 Digital Signatures

Given the characteristic that only the entity that has the private key can encrypt with it private key knowledge can be utilized as an authentication method. This is a common practice known as a digital signature. Similar to a checksum, a digital signature

is created by first compressing the message that is intended to be signed through a hashing algorithm, also known as a message digest. A digital signature is the encryption of the message digest using the private key of the sender. Figure 2-4 below illustrates this system.

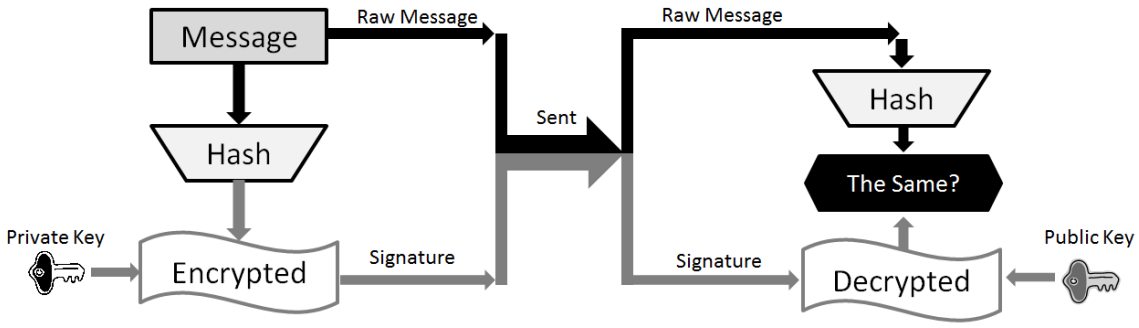

Figure 2-4. Illustration of digital signature scheme. Note that both the raw message and the signature are sent across the network.

As shown above, the signature is sent along with the plaintext of the message. After the decryption of the signature with the sender's public key the receiver is confident of who sent the message (authentication). The receiver also performs the same digest on the raw message and checks the one that is in the signature. If they match the receiver is also confident of the content of the message (integrity) [6] [19].

2.3.2 PKI

One detail noted above is actually a very important and difficult aspect to public key cryptography – making sure everyone has access to the correct, updated, and validated public keys they need. This objective is achieved through implementation of a PKI. As explained in [6] a PKI consists of "certificates, a method of revoking certificates, and a method of evaluating a chain of certificates".

Certificates are messages which contain an entity's identification information, certificate specific information such as expiration date, and, most importantly, its public key. Certificates are signed with a trusted authority's private key and are sent in the open

to whoever needs them. When a node receives a certificate it can decrypt it using the trusted authority's public key and access and trust the information contained inside. Now that node can decrypt messages from the certificate's owner and trust that it has the correct public key. In the context of this paper, certificates are given to aircraft and ATC centers so they can send them to those that require the knowledge of their public key [6].

A PKI requires a chain of trust where each node that receives a certificate has all the certificates for the entities which signed that certificate, eventually leading up to a trusted authority. For the system to be secure everyone has the trusted authority's public key and the authority's private key has not been compromised. The entities which are responsible for securely disseminating certificates through encrypting them with their own private keys are known as certificate authorities (CA). The assumption is that the receivers of the certificates trust the CA which sent them and that the CA's private key is kept secret. In the context of this paper the CA is the FAA.

There also needs to be an efficient way of terminating a certificate's validity, otherwise known as revocation. There are a number of methods in which certificates are revoked; some just as simple as telling everyone who has that certificate to stop using it. However this can be inefficient and sometimes insecure. Typically, if the overall number of certificates is small, the best way to handle certificate revocation is to have a certification revocation list (CRL) [6]. This list is maintained by the CA and is updated and disseminated to those who use the certificates. When a user receives a new certificate it checks the CRL to make sure that it has not been previously revoked [6]. In terms of this paper the CRL is maintained by the FAA and disseminated to the ATC centers.

The concepts discussed above are used in comparable domains to address similar issues. To determine what research has been done in these areas a literary review of proposed designs is required. The following section discusses these domains, the issues that they present and what designs are proposed to solve them.

2.4 Related Works

The following section describes a few research areas which present similar issues to those suggested in section 2.2.4. Vehicular ad hoc networks (VANETs) are similar in structure and present characteristics and issues that the aviation domain has. However, some designs focus on different security objectives and assume different infrastructures and resources. These similarities and differences are discussed in more detail in this section along with a brief discussion on what research has been done in the area of ATC and data communications security.

2.4.1 VANETs

Research into security in vehicle-to-vehicle (V2V) communications in VANETs can provide perspective on how to go about solving the issues which ATC communication systems have. The assumption most researchers make is that in the near future vehicles will have the ability to communicate using wireless communication using the same techniques as ADS-B [21] [22] [23]. This will have a similar effect on the system as well; cars will be able to get closer together at higher speeds which in turn will increase overall system efficiency and safety. Many of these systems have characteristics which push more towards efficiency and low overhead [21] [24]. However, many researchers discuss the need for robust security measures to handle the potential threat of malicious attacks to the system [22] [23] [25] [26]. The similar issues between VANETs and the ATC domain include all the aspects of a robust PKI: having a trusted CA, a method for evaluating certificates, and a method for revoking certificates. Each one of these is discussed in the following paragraphs.

Having a trusted CA is crucial to the successful implementation of a PKI. In the VANET domain some have suggested an overarching CA that handles the entire system [23] [27]. Some have suggested reducing the workload of the CA by employing a "self-authorization" scheme [28]. Others have proposed to completely take the CA out of the system and use a group-verification process where each automobile authenticates all the ones around it [29]. However, unlike the ad hoc nature of VANETs and V2V

communication systems the NAS provides robust infrastructure as well as the FAA which can act as a known and trusted authority who regulates all air traffic.

Certificate revocation is a difficult task in both the VANET and ATC domains. Many VANET researchers have suggested ways of efficiently disseminated CRLs to all vehicles in the network using compression techniques and a push delivery mechanism [23] [27] [30]. These techniques require the CA to send the CRL and the cars to process them; only then can each node be made aware of whether other nodes around them are valid or not. Some have even proposed a car-to-car forwarding technique of the CRL to gain efficiency [28]. All these techniques are based on the infrastructure-less VANET domain. Luckily, the aviation domain has a strong infrastructure like the one described in FTI and can be utilized to disseminate the CRL to ATC centers across the country. This process is described in further detail in section 4.3.

The next step it so look into the state of the art of ATC PKI designs. This literary review is done to determine what research has been done in the area. After determining what progress has been made it can be more clear what additional research needs to be done. The next section discusses the state of the art of ATC PKI designs and what advances have been made in the research area.

2.4.2 State of the art: "ATC PKI" Designs

There have not been many proposed cyber security related designs to handle the issues of secure data communications in the NAS. A search on the American Institute of Aeronautics and Astronautics (AIAA) and Institute of Electrical and Electronics Engineers (IEEE) archives for "air traffic control" and "PKI" returned less than a dozen papers related to this research. Some of them present simple PKI designs to handle distribution and revocation of certificates typically breaking out the communications by ground-to-ground or air-to-ground [2] [3]. Some suggested digital signatures as a method for integrity protecting messages but left out key components such as how the PKI would utilize the current systems available at ATC centers today [31]. There is also a strong emphasis on validation due to the ad hoc nature of aircraft communications [3][4].

However, these designs do not take advantage of the natural aircraft registration process or the role that ATC centers plays in the identification and monitoring of aircraft.

This chapter described the current system in which aircraft are identified and monitored by ATC and explicitly states the gap in knowledge. Cyber security primitives are discussed along with current research in similar domains. This lays out the necessary information required to understand the domain and the tools to be used in the design. Next the problem definition is formalized using requirements along with a comprehensive attack model.

Chapter 3
Problem Definition

As noted in the previous section, there are a few security issues with the current data communication system between aircraft and ATC. Considering the contemporary cyber security techniques discussed, public key cryptography, digital signatures and PKI, there are tools that can be utilized to potentially solve some of these issues. First, the issues need to be formalized into security objectives so the correct implementation of these techniques can be determined. This section discusses these security objectives along with the potential attacks the system might face.

3.1 Security Objectives

The following section discusses the security objectives required to close the gap in knowledge stated in the previous section. This section lists requirements needed to achieve aircraft and ATC authentication along with integrity protection for each message broadcasted from aircraft. Following the requirements is an attack model which lists potential attacks that will need to be mitigated by the design.

3.1.1 Authentication

As discussed in Chapter 2, confidently determining the identity of an aircraft is difficult. Most methods employed by ATC use combinations of radar, radio, and messages broadcasted from aircraft to accurately determine each aircraft's identification. However, in the presence of a malicious attacker, these methods are not enough to completely ensure identity. In order to appropriately mitigate potential attacks, authentication of broadcasted messages from aircraft and ATC needs to be a major security objective. In the context of this paper, authentication is defined in three ways:

1. *All ATC centers shall confirm the identity of what aircraft they are receiving data from*

2. *All aircraft shall confirm the identity of what ATC center they are receiving data from*
3. *All aircraft shall confirm the identity of other aircraft they are receiving data from*

3.1.2 Integrity Protection

There is also the potential for attackers to manipulate information within each message that is sent. Considering that the information contained in each message from aircraft and ATC are important to the overall function and safety of each flight, each receiver needs to be absolutely sure that the data they receive is received as intended. This concept is known as content integrity. It is also important to consider message source integrity which is the ability to accurately determine who sent each message. In the context of this paper, integrity protection is defined in the following ways:

1. *The receiver shall have complete confidence that the information in each message has not been manipulated in any way*
2. *The receiver shall be able to immediately determine if the contents of each message have been manipulated.*
3. *The receiver shall be able to immediately determine if the contents of each message was sent by an authenticated source.*

3.2 Attack Model

Now that the security objectives are laid out, the potential attacks on the system need to be defined. These attacks will be discussed later as to how the design accomplishes the mitigation of the threats.

1. *Replay Attack:* Assuming that messages are signed with private keys and are available for anyone to collect, someone could try to replay some of these messages at a later time and fool ATC or other aircraft. A potential scenario, as

shown in Figure 3-1, an attacker creates several "ghost" aircraft, say on a runway at an airport, which may cause serious security and safety issues.

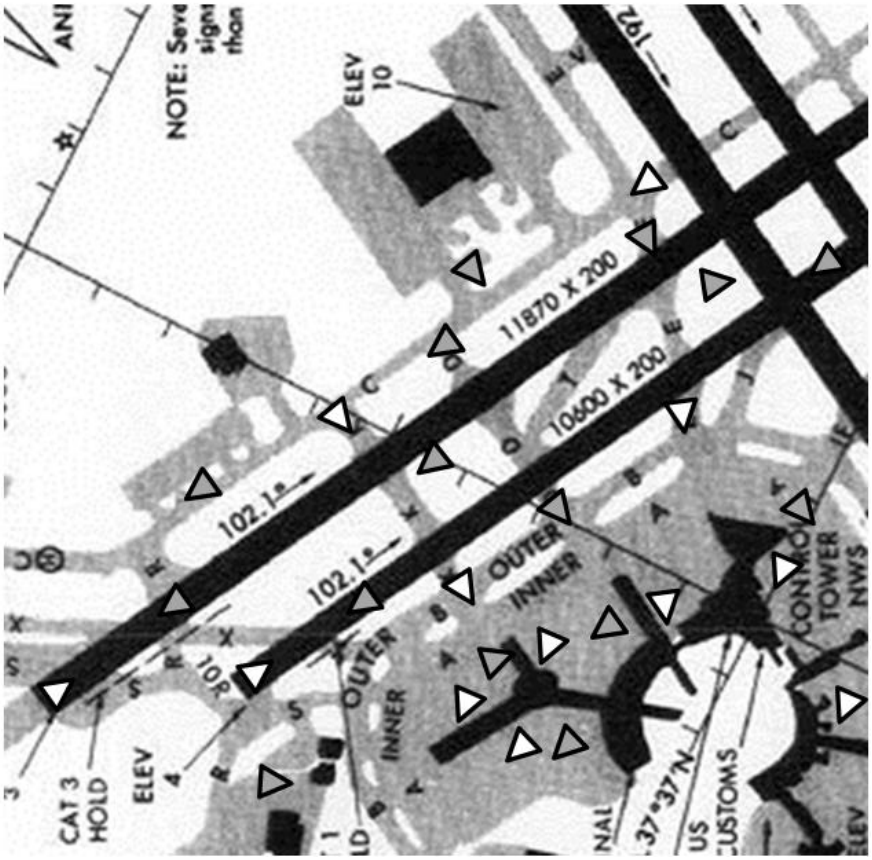

Figure 3-1. A airport map showing real targets (white) and "ghost" targets (grey). In this situation, a malicious attacker may create many "ghosts" to confuse ATC and other aircraft

In Figure 3-1, ATC could suddenly start getting messages that were sent in the past with valid signatures. This could be done by replaying many old messages that the attacker picked up while listening to raw data communication between ATC and aircraft on the ground.

2. *Modification Attack*: If one was trying to maliciously manipulate the message content they may only want to slightly move where the aircraft says it is. In parallel arrival and departure situations it would not take much movement of the aircraft supposed location to cause some serious issues. This situation is illustrated in Figure 3-2 where ALC456 and BOB123 are on a parallel approach.

An unknown entity manipulates ALC456's message content and moves the aircraft much closer to BOB123. This can cause serious safety concerns.

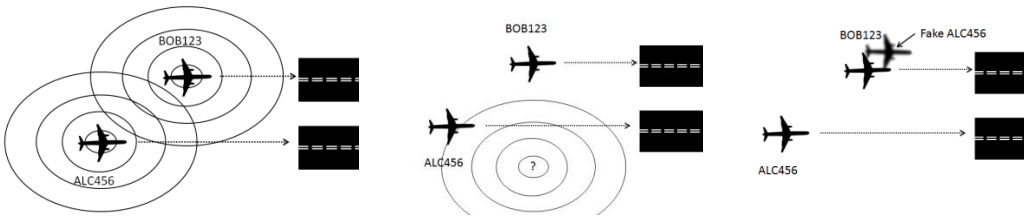

Figure 3-2. Two aircraft on approach on parallel runways. Attacker manipulates ALC456's messages to move dangerously close to Bob

Figure 3-2 shows a special situation where aircraft are "paired" together during parallel takeoffs and landings. During these operations ATC needs to be involved in the pairing and the authentication of each aircraft [1] . This situation is discussed in more detail in the next chapter.

3. *Man-in-the-Middle Attack*: This is when an intruder collects information between two communicating parties in an attempt to cause one of them to reveal a secret. In the case of aircraft-to-ATC or aircraft-to-aircraft authentication an intruder would try to determine a weakness in the system in order to take advantage later.

4. *FAA Insider Attack.* Keeping the private key of the CA secret is tantamount to the security of the entire system. If an attacker is someone at the FAA who has access to its private key and starts signing fraudulent certificates then anyone using them would be completely fooled. This attack will need to be mitigated by secondary security systems in the design.

5. *ATC Insider Attack*: ATC has a considerable amount of power considering they are the primary source of information about traffic in the area which they preside. The design will need to address the vulnerabilities which will arise if ATC's key is compromised and present the ways in which as many of them can be mitigated as possible.

6. *An Aircraft's Private Key is compromised:* Someone else can sign raw messages with another aircraft's private key. This will most likely require interaction by ATC to mitigate the risks involved.

7. *The CRL is compromised:* Someone modified the CRL to remove or add certificates.

Each of these attacks needs to be explicitly mitigated by the design described in this paper. After a thorough explanation of the design in Chapter 4, Chapter 5 will provide adequate proof that each attack is prevented when the proposed system is in place.

Chapter 4
Dual Path PKI (DPP) for Secure Aircraft Communication

The most important aspect to secure aircraft-to-aircraft and aircraft-to-ATC communication is having a robust PKI. Such a system requires a few important components including trusted CAs, certificate design, methods for evaluating and revoking certificates, strong protocols for authentication and mechanisms to provide integrity protection. The following sections describe these aspects of the design to accomplish the requirements set in the problem definition.

4.1 Certificate Authority (CA)

In any robust PKI design there needs to be a well-defined and trusted CA. There are a few possibilities for CAs in the domain of aviation to consider such as airlines or operators, ATC centers, and the numerous government authorities which handle ATC operations, safety, and security. However, considering that aviation is well regulated within the United States, the FAA is the obvious choice for the CA. It not only presides over the entire ATC system, it regulates each aircraft by requiring documentation and licensing [32]. Therefore, for the DPP design the FAA will be the overarching CA for all entities and will have a secure private key which it will use to sign certificates for aircraft and ATC centers. Considering the dual nature aspect of the design, ATC centers will act as local CAs and will have the capability to sign session certificates for aircraft in the area they control.

It is important to note exactly why there are two paths through which aircraft receive certificates. A significant aspect of a robust PKI design is how participating entities become aware of the revocation of others' certificates. Most designs have the CA hold the CRL and require nodes to perform the check. This requires each node to have

access to the entire CRL which can cause issues with available bandwidth. Considering the bandwidth constraint of direct aircraft communications and the limited processing power onboard each aircraft it would be advantageous to have ATC check the CRL. The DPP design accounts for this through the development of an aircraft session certificate which is given to the aircraft by the local ATC center only once the CRL has been checked. This reduces bandwidth consumption, redundant processing by each aircraft, and increases the validity of certificates by making them session dependent. It also puts more responsibility of validating aircraft certificates on the local ATC center which makes sense considering the secondary systems that ATC has access to. These short term session certificates along with long term certificates are discussed in greater detail in the next session.

4.2 Certificates Design

This section describes the contents of the certificates which are assigned to ATC centers and aircraft. The FAA signs certificates for both ATC centers and all registered aircraft. ATC centers receive certificates from the FAA so they can verify and disseminate their public keys. Considering the dual path aspect of the design each aircraft has the opportunity to get certificates from both the FAA and the local ATC center that they are currently in. This double certification proves that each aircraft has been granted the ability to fly in the NAS (the long term FAA certificate) and validated as a safe and current entity within the local center it is flying (the short term ATC session certificate). This structure is illustrated in Figure 4-1 below.

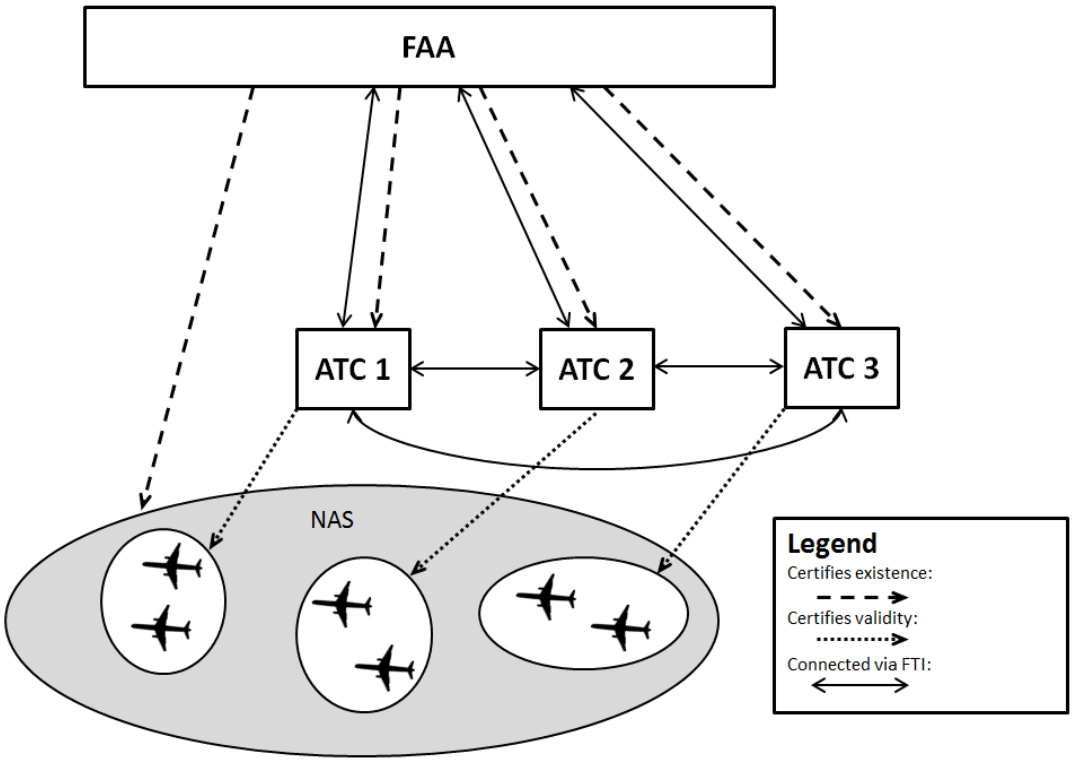

Figure 4-1. The Dual Path PKI for Secure Aircraft Communication architecture

The contents of each of these certificates are described in the following section.

4.2.1 FAA Certificates

When an operator registers an aircraft with the FAA it is required to submit information that is specific to the aircraft such as registration number, aircraft make, model and series, and a serial number that was assigned to the airframe when it was built. Consider the registration number of an aircraft being analogous to a license plate number of a car. An operator files operations specifications (OpSpec) using this information which "include the terms, conditions, and limitations reasonably necessary to ensure safety in air transportation" [32]. OpSpecs allows the FAA to uniquely identify an aircraft by operator and know what it has been authorized to do. In order to uniquely identify a message that is sent by an aircraft's transponder each aircraft is also assigned a Mode-S number when built [1]. The DPP design has the FAA gather this information and create a long term certificate which it signs and delivers to each aircraft. This certificate is created with the intention of remaining valid until the aircraft is bought,

sold, retired, or destroyed. Below is a list of the contents of a certificate granted by the FAA to a registered aircraft:

1. N-Number (Registration Number): unique to an aircraft only at a certain point in time
2. Mode-S Code (Transponder Code): known to be permanently unique to an airframe
3. Expiration Date: Long term expiration date, typically many years
4. Public Key

All this information is kept in a secure FAA database. The certificates will be made available to all ATC centers through FTI which interconnects all entities necessary to the functions of FAA and ATC [12].

ATC centers will also need to get certificates from the FAA so they can disseminate their public keys to other ATC centers and aircraft in their area. To uniquely identify an ATC center their 3-letter location indicators established by the International Civil Aviation Organization (ICAO) [33] [34], are used. Below is a list of the contents of a certificate granted by the FAA to each ATC center:

1. ATC Center 3-letter identifier
2. Expiration Date: Long term expiration date. Typically many years
3. Public Key

ATC centers are rarely created, destroyed, or require an ICAO identifier change. Therefore each certificate is created with the intention of being long term. The next section describes session certificates that are short term.

4.2.2 ATC Session Certificates

ATC also assigns session certificates to aircraft in their region. These certificates are very similar to the FAA certificates and are granted after the ATC center verifies the aircraft's certificate has not been revoked by the FAA. Note that timestamp+1 is used as validation for the aircraft who requested the certificate. The specifics of how the certificate is used during authentication are discussed later in this chapter. The list below states the design of the certificate given to aircraft by the local ATC center:

1. N-Number (Registration Number): unique to an aircraft only at a certain point in time
2. Mode-S Code (Transponder Code): known to be permanently unique to an airframe
3. Expiration Date: Short term expiration date. Typically less than an hour
4. Timestamp+1
5. Public Key

These session certificates are created with the intention to last only a number of minutes until the aircraft has landed or is handed off to another controller. They verify an aircraft's long term ticket and solidify their existence within an ATC center's region of responsibility. This is done primarily to prevent someone from using a revoked certificate. The next section discusses why session certificates were chosen over other potential designs.

4.2.3 Why Session Certificates

The long term FAA certificate validates the existence of an aircraft but it does not replace the ATC's involvement in the short term validation of an aircraft's whereabouts. Several mechanisms were considered as ways to handle the short term verification of an aircraft's long term certificate, including session keys or group keys between aircraft. However, the domain characteristics need to be considered before a design is determined. ADS-B is a broadcast based communication mechanism. This means that any key management scheme needs to allow for several entities to authentication and integrity check several other entities messages. Session keys are not appropriate as they require several message passes to create and each key is specific to a pair of aircraft. The dynamic nature of the ATC environment and broadcast dependent ADS-B messages would not allow for the successful implementation of group keys. Therefore, basic asymmetric key methods are chosen; each entity authenticates other entities using the basic concepts of public/private key encryption. This only requires the public key itself to be validated at the time of aircraft authentication. The session certificate concept was chosen to provide short term validation of an aircraft's public key. As mentioned above, the session certificate is meant to handle the difficult task of making sure an aircraft's

long term certificate has not been revoked. The next section discusses the certificate revocation process for this design and why it is a key component of a robust PKI.

4.3 Certificate Revocation

An important aspect to PKI design is an efficient way of revoking certificates. Without a well-defined way for entities operating within a PKI to have knowledge of what certificates have been revoked, attackers could reuse revoked certificates in an effort to gain authorization into the system. The number of entities requiring certificates in the aviation domain is relatively low, therefore the DPP design proposes a master CRL list which contains all the certificates which are revoked. Considering that the FAA is the all-powerful CA they hold and maintain this CRL. Aircraft certificates are revoked for a number of reasons: 1) an aircraft retiring, 2) an aircraft being parked for a long period of time, 3) an aircraft changing operators which will change their N-Number, 4) an aircraft is destroyed or 5) any other reason that the information inside the certificate changes. The FAA has a direct data link with all ATCs through FTI [12] [13] which allow each center to have a consistent list of revoked certificates.

Aircraft will have a harder time getting access to the most recent CRL because of their mobile ad-hoc nature where they can only access the FAA database when they are on the ground. Considering that all aircraft need to be validated by the local ATC, the center will take on the responsibility of checking the CRL and notifying aircraft in the area if other aircraft are valid. This is done through the utilization of the session certificate discussed in section 4.2.2 above. This concept is described in greater detail later in this section.

4.4 Certificate Evaluation

After the certificates are given to each aircraft and ATC center there needs to be a formal way in which they are evaluated when received by others. There are two main evaluations: 1) evaluating an aircraft's certificate and 2) evaluating an ATC center's

certificate. Both certificates are signed with the FAA's private key. This makes evaluation relatively simple. Anyone who wishes to access information inside an entity's FAA certificate simply needs to decrypt it using the FAA's public key. Anyone who wishes to access information inside an aircraft's ATC certificate simple needs to decrypt it using the ATC center's public key pulled from its FAA certificate.

4.5 Aircraft Message Signature

It is important to note that the messages broadcasted by aircraft might not require authentication and integrity protection. Quite the contrary, most interested parties do not care who the messages come from. This is because the FAA, ATC, and other aircraft might just want to get a basic picture of who is flying where. This thesis proposes a solution which can be bootstrapped into the current system. A significant feature of this is making sure aircraft and ATC centers who do not wish to take part in the secure system proposed in this paper can still gain access to broadcasted messages. This is why a digital signature scheme is proposed.

Each message broadcasted from the aircraft contains many fields. Table 4-1 lists the data passed in each message important to mention for purposes of this paper [10]:

Table 4-1. ADS-B Message Structure **[10]**

Data Item	Length in Bytes	Criteria for Inclusion: A=Always, O=Optional
Link Technology Indicator	1	A
Time of Applicability	4	A
Target Address	4	A
Integrity/Accuracy Parameter	3	A
Latitude/Longitude	6	A
Pressure Altitude	2	A
Velocity (Airborne)	5	O
Velocity (Surface)	4	O
Modes and Codes	2	O

Many fields in ADS-B messages are optional and some are broadcasted less often than others. There are several ADS-B message formats which vary in length [35]. For purposes of this paper the long message of 32 bytes will be assumed. The message length is important to the performance evaluation of the design regarding how long it takes to sign each message.

All ADS-B broadcasts will still be sent in the clear. However, to add authentication and integrity protection a digital signature is utilized. As described in section 2.3.2, a digital signature is a digest of the raw message encrypted with the sender's private key. The message architecture is illustrated in Figure 4-1 below.

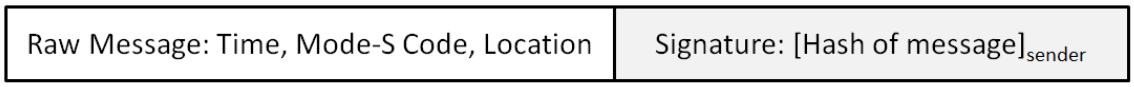

Figure 4-2. A breakdown of each broadcasted message

4.6 Authentication Protocols

The following section describes the authentication protocols employed so that aircraft and ATC can mutually authenticate each other. The meticulous design of these protocols is essential to the security of the entire system.

4.6.1 ATC-to-Aircraft Mutual Authentication

In this scenario an ATC center XYZ is assigned aircraft A and is going to begin receiving signed broadcast messages from it. A robust interrogation and response protocol is employed so that both aircraft A and center XYZ can authenticate each other. Aircraft A is constantly broadcasting messages containing its N-Number with a specific transponder code along with a signature so center XYZ already has access to the information it needs to pull the correct certificate. Center XYZ queries the FAA's database through FTI and pulls the certificate with that transponder code and N-Number combination then checks the CRL to make sure the certificate has not been revoked.

At this point XYZ has access to a valid and current public key for aircraft A. Center XYZ can then authenticate and integrity check all of aircraft A's messages. However, aircraft A has not authenticated center XYZ. To accomplish this center XYZ encrypts aircraft A's identification information, the original message's timepstamp+1, along with an expiration date and returns this to aircraft A. Note that the expiration date is expected to be relatively soon after center XYZ is no longer responsible for aircraft A and subsequently cannot validate its certificate. Aircraft A decrypts the message and can authenticate center XYZ through comparing the timestamps and the assumption only XYZ can encrypt with its private key. Figure 4-3 below illustrates the messages that are passed between ATC and the aircraft in order for center XYZ and aircraft A to mutually authenticate.

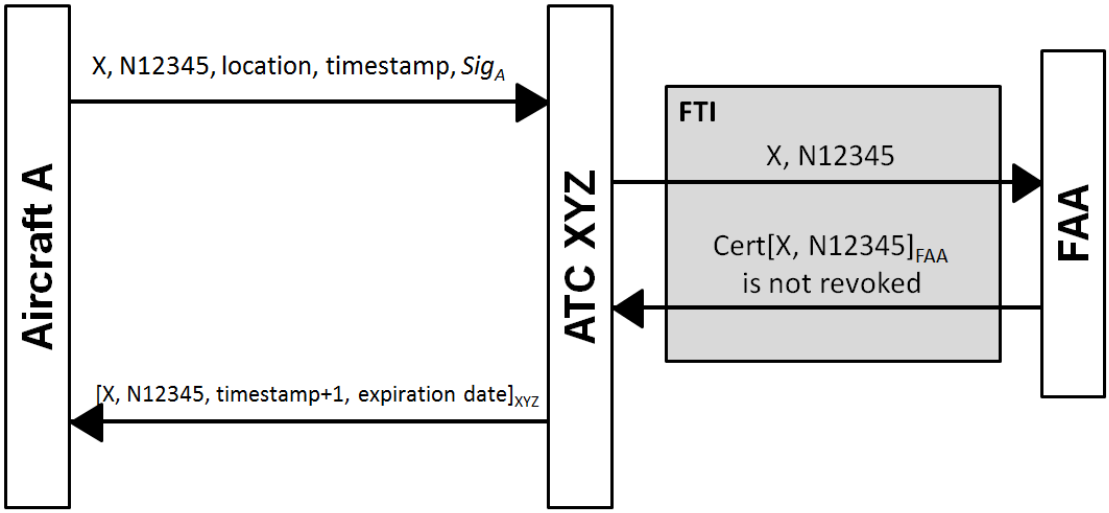

Figure 4-3. Mutual ATC to aircraft authentication protocol

Now the aircraft has a certificate signed by center XYZ. This new certificate is purely authenticated by the local ATC center. The main reason to have the local center sign the ticket is due to ATC having a constant connection to the FAA's revocation database. Once an aircraft's ticket is validated by the local center, other aircraft who receive that ticket can be sure that it is not revoked. This concept is explained further in the next section regarding aircraft-to-aircraft mutual authentication.

It is important to note that aircraft and ATC must have synchronized clocks in order to prevent the issues with large time skews. The larger the difference in times onboard the aircraft versus at the local ATC center the higher risk each entity has for malicious attacks to the system, such as replay attacks [6]. Synchronized clocks are also important in the aircraft-to-aircraft mutual authentication scheme described in the next section.

4.6.2 Aircraft-to-Aircraft Mutual Authentication

In most situations aircraft can rely on ATC to authenticate and integrity check the messages coming from the aircraft around them. This is actually analogous to how aircraft monitoring has worked since ATC's inception. In situations where aircraft are much closer to each other, i.e. during parallel departures and arrivals, it is more efficient for the aircraft to take on the responsibility of maintaining separation. If aircraft can authenticate and integrity check each other's messages, this can reduce the workload taken on by ATC and potentially reduce separation through reduction in communication delays. However, it would be wise to keep ATC involved in the initial authentication protocol to increase overall system security and integrity.

In order for aircraft A to authenticate another aircraft B it needs to gain access to its public key. Considering that aircraft are not sure who they will want to authenticate and are not always connected to an FAA database when they are in the air, it makes sense to utilize ATC's secure connection to gain access to valid certificates. Assume that both aircraft A and aircraft B have already completed their mutual authentication protocols with ATC center XYZ, described in section 4.6.1 and illustrated in Figure 4-2, and have new session certificates. Now the aircraft have everything they need to authenticate each other.

Aircraft A broadcasts its message along with the session certificate it received from XYZ. Aircraft B receives the message and checks the validity of the certificate by decrypting and checking the expiration date. If the certificate is valid, it then checks the validity of the original position and identification message by checking the signature

block with the public key found in the certificate. If that checks out, then it broadcasts its session certificate along the next original message.

When aircraft A receives the certificate it checks its validity by making sure the expiration date has not passed. If the certificate is valid, it then checks the validity of the original position and identification message by checking the signature block. If the signature block is valid, then aircraft A has now authenticated aircraft B because of the assumption that only aircraft B can encrypt with its private key. Figure 4-4 below illustrates the mutual authentication between aircraft A and aircraft B.

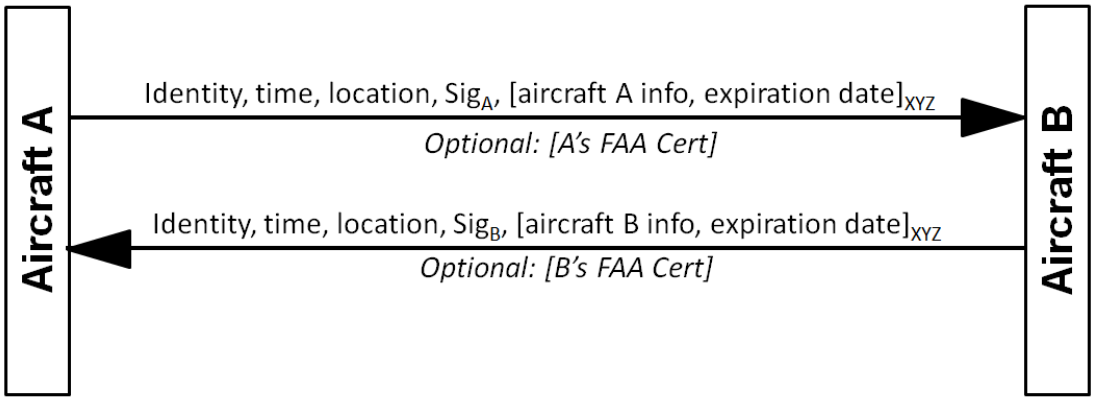

Figure 4-4. Aircraft-to-aircraft mutual authentication protocol

Once the aircraft have performed the mutual authentication protocol shown above they can know for sure who they are sending messages to and receiving messages from. Note the "Optional" FAA certificates that aircraft A and B can send each other. This is if they have any doubt in XYZ's validity they can do a double check with their FAA certificates. This optional message is to mitigate certain risks including the possibility of the local ATC center's private key being compromised.

The next section takes the components of the design discussed in sections 4.1 to 4.6 and applies them step by step to explain exactly how the design would work if implemented in the real world.

4.7 Design Application

Considering the domain of the DPP design it makes sense to include a step by step explanation of its application. The following sections detail the application of the design broken out by the following steps: 1) aircraft is manufactured; 2) pre-flight preparation; 3) secure parallel departure procedure; 4) secure ATC handoff operation; 5) secure parallel arrival procedure.

4.7.1 Aircraft is manufactured

When an aircraft is first manufactured it is given a number of specific attributes that it will keep throughout its lifetime. The manufacturer assigns a model and series to the aircraft based on when it was made. Also, a unique Mode-S transponder code is assigned to the aircraft so that any tower that utilizes the ATRCRBS can identify the aircraft. Further, the operator to which the aircraft is sold assigns a unique N-Number. Note that N-Numbers are only unique at a particular time; as an aircraft is bought and sold the new owner assigns the aircraft a new N-Number [1] . Once the aircraft is ready to operate within the NAS, the operator files it with the FAA. The FAA will grant the operator the right to operate the aircraft and also assigns the aircraft a certificate which is detailed in section 4.2. The aircraft now has everything it needs to operate safely within the NAS.

4.7.2 Pre-flight preparation

In preparation for each flight aircraft file a flight plan with the FAA [1] . This flight plan consists of a number of fields including aircraft identification information like N-Number, make, model and series of the aircraft, and the operator. It also has operation specific information like arrival and departure airports and route information including which control centers it will fly through. These flight plans are filled out and disseminated to all ATC centers which might require the information. This provides a perfect mechanism to reference which ATC center's certificates each aircraft will require throughout the flight. When the ATC center receives the departing aircraft's flight plan it referencing the route information to determine the certificates the aircraft needs. The

center uses the FTI to query the ATC center certificate database by their designators. The center also checks the FAA's master CRL to assure none of the center's certificates have been revoked. If these steps are completely appropriately it is safe to assume that the aircraft has the correct certificates for each center on board during flight.

There is an important assumption that during the flight none of the ATC center's certificates are revoked. Considering that ATC centers rarely change there will be few changes to the certificate database. It is safe to assume that if there are changes the FAA will make them in a timely manner so that flights that are in progress will not be affected.

4.7.3 Secure Parallel Departure Procedure

One way that the FAA has decided to increase efficiency and throughput at many airports is by designing and implementing procedures that allow aircraft to depart next to each other on parallel runways [5]. Several airports in the country have closely spaced parallel runways, less than 4,300 feet apart, and require the aircraft to maintain safe separation [5]. Considering how close the aircraft get it is difficult for ATC to be involved in constantly maintaining separation. This proposal's implementation of aircraft-to-aircraft communication can help with this challenge if the messages sent between aircraft are secure. This section describes how aircraft can authenticate and integrity protect communication between each other so that they can safely depart an airport on parallel runways.

As two aircraft prepare to take off they both begin broadcasting data. These messages include identification, location, and signature blocks as discussed in section 4.5. The nearby ATC center begins receiving messages from both aircraft and they each complete the mutual authentication protocol outlined in section 4.6.1 through which they both receive session certificates. After completing the authentication protocol all messages that are broadcasted by the aircraft can be authenticated and integrity checked by the local ATC center. This is illustrated in Figure 4-4 below.

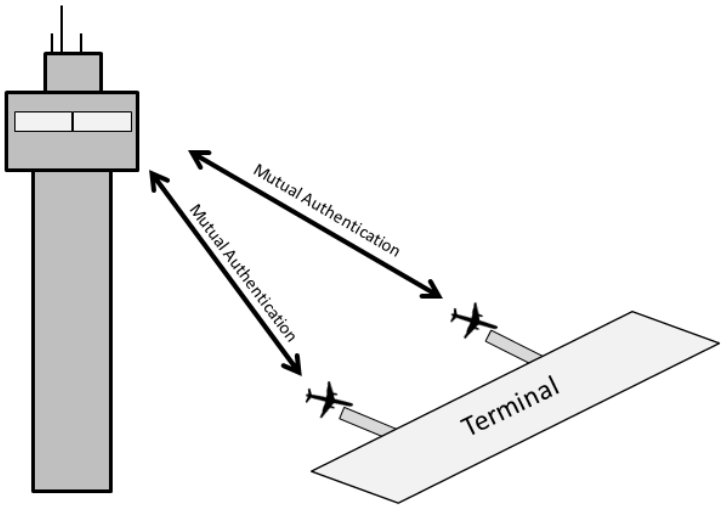

Figure 4-5. Two aircraft mutually authenticate with the local ATC tower

ATC then pairs two aircraft for parallel departure. Typically airports decide to pair aircraft when traffic is heavy and they base the pairing on aircraft weight class and performance to mitigate other risks, such as wake avoidance, involved with parallel departures [35]. After being paired the aircraft need to mutually authenticate each other so they can integrity check all the messages they receive. This protocol is described in in section 4.6.2. This process is completed as they line up for takeoff and illustrated in Figure 4-6 below.

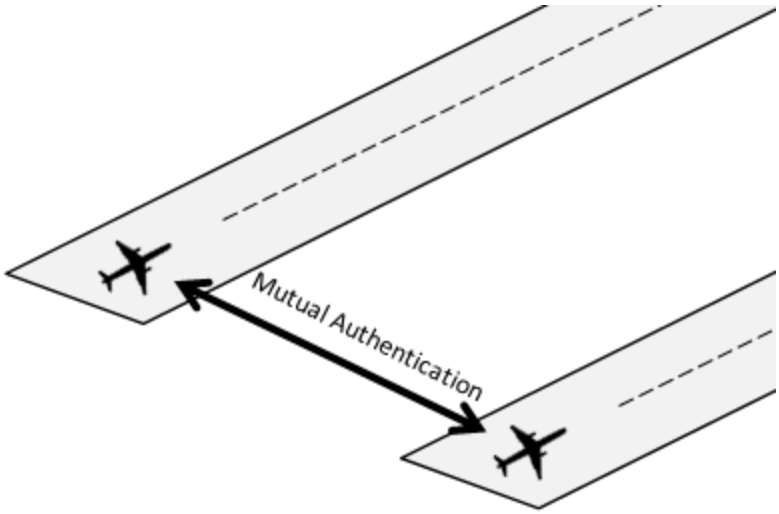

Figure 4-6. Two aircraft mutually authenticate with each other before parallel departure

Once the aircraft have mutually authenticated each other they can be sure who they are talking to and that messages have not been manipulated. This allows for secure communication between the aircraft as they depart.

4.7.4 Secure ATC handoff procedure

As an aircraft proceeds to its final destination it may be required to travel through a different ARTCC or TRACON from the one it took off from. This will require the current ATC center to handoff responsibility of monitoring that aircraft to another ATC center. Through FTI, all centers have access to aircraft and other ATC centers' certificates and all centers are securely interconnected. This allows for the safe passage of information between centers.

Before an aircraft leaves the terminal it files a flight plan which includes all ATC centers that it will fly through. Each center is then notified of the aircraft's intention to enter the center's airspace at some point in the future. This allows the center to be prepared for the aircraft's arrival by accessing the FAA's certificate database ahead of time to pull required certificates.

Assuming that the aircraft is authenticated by the initial center using the protocol described in section 4.6.1, it has a session certificate signed by that center. Once an aircraft is about to cross the ATC center boundary the initial center notifies the new center of the aircraft's entry through FTI. All the aircraft is required to do is send its current session certificate to the new center. The new center can access the initial center's certificate to get its public key and decrypt the aircraft's session certificate. If the expiration date has not passed then the center knows the aircraft is verified by the initial center. The new center now sends a new certificate to the aircraft with a new expiration date. This procedure is illustrated in Figure 4-7 below.

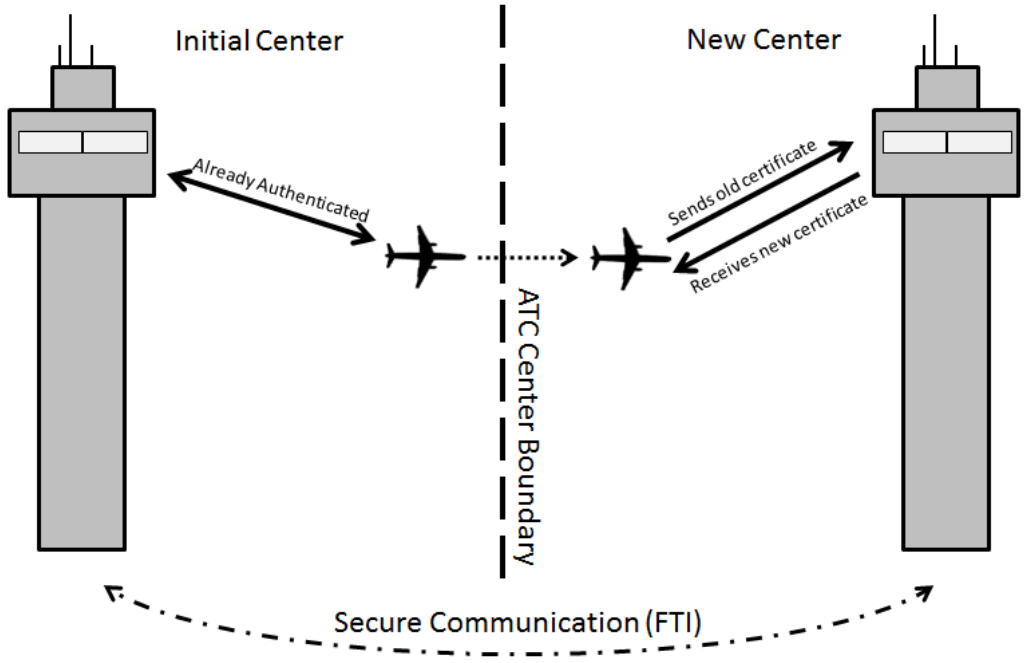

Figure 4-7. Secure aircraft handoff from initial ATC center to new ATC center

Once the aircraft receives the new certificate from the new ATC center it can use that certificated to mutually authenticate other aircraft in the area. An example of this is the secure parallel arrival procedure which is described in detail in the next section.

4.7.5 Secure Parallel Arrival Procedure

Similar to the procedure described in section 4.7.3, the parallel arrival procedure is when aircraft line to up land next to each other on parallel runways. This has a similar

effect as the parallel departure as it increases airport efficiency and throughput. When ATC decides to execute parallel arrivals it pairs up aircraft in the terminal area. Assuming that each aircraft has already authenticated with the center using the protocol described in section 4.6.1, each aircraft should have a session certificate. These certificates can then be used to mutually authenticate aircraft that are pairing up to land using the procedure described in section 4.6.2. This procedure is illustrated in Figure 4-8 below.

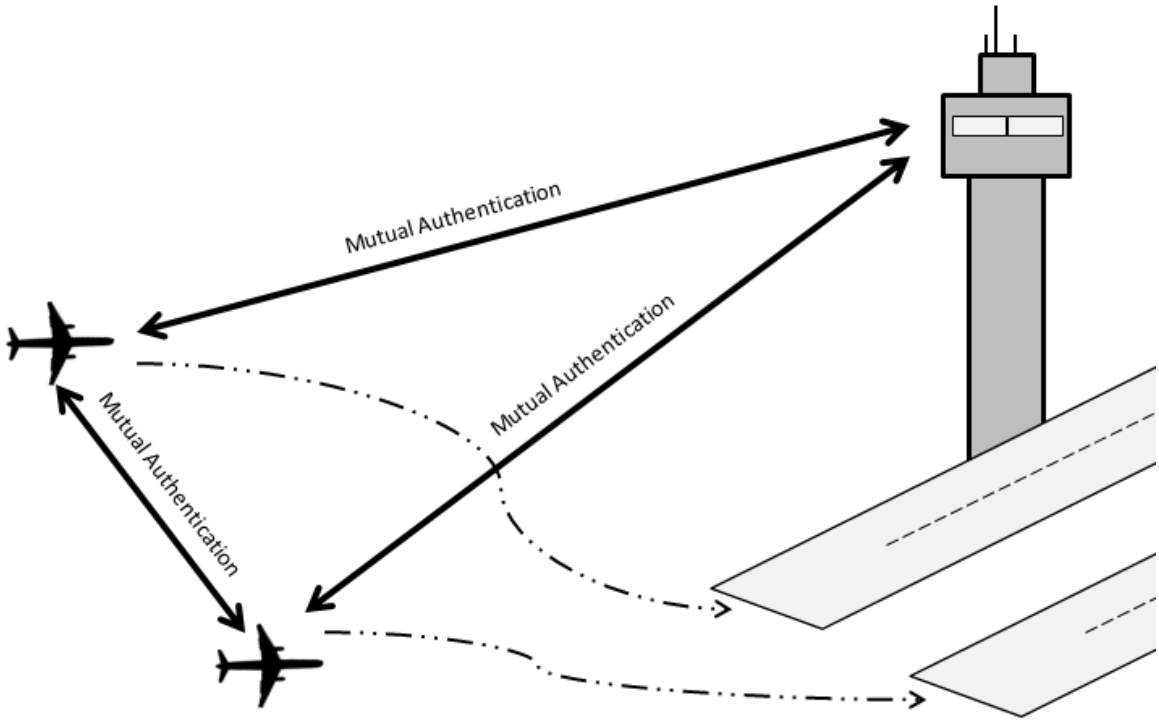

Figure 4-8. Secure paired arrival procedure

Once both aircraft have mutually authenticated each other they can proceed with the parallel arrival procedure with accurate and valid communications.

This chapter described the DPP design through the protocols and procedures required for it to accomplish the requirements set in Chapter 3. The next chapter explicitly states how each requirement is met and how each potential attack is mitigated.

Chapter 5
Security Analysis

This section describes how the DPP design accomplishes all the requirements and mitigates all the attacks expressed in Chapter 3. In the next couple of sections each of the requirements expressed in section 3.1 will be addressed. After it is proven that each requirement is met there is a discussion on how each potential attack is mitigated.

5.1 Authentication

There are three requirements for authentication. This section lists them out and explicitly states how each one is met through the design explained in Chapter 4.

1. *All ATC centers shall confirm the identity of what aircraft they are receiving data from*

   Each ATC linked with the FTI can verify that each aircraft certificate has not been revoked. Once the aircraft's ticket is verified the center can then be sure of the aircraft's public key. Through completing the ATC-to-Aircraft Mutual Authentication protocol described in section 4.6.1 the ATC center authenticates the aircraft through decrypting the aircraft's message signature which reveals the digest of the raw message. Then the center performs the same message digest on the raw message that was sent from the aircraft. If the digest in the signature matches the digest computed by the center then the center can be completely sure of the aircraft's identity. However, the validity of the authentication relies on the aircraft keeping its private key secret. Mitigating this risk is discussed later when each potential attack is discussed.

2. *All aircraft shall confirm the identity of what ATC center they are receiving data from*

Aircraft gather the ATC centers' certificates it needs before takeoff through the local center's connection with the FAA's certificate database via FTI. Assuming that each certificate is valid the aircraft can assume that it has all the public keys necessary to authenticate each ATC center it passes through. Similar to the first requirement, the aircraft authenticates each ATC center by completing the protocol described in section 4.6.1. The aircraft can be sure of the ATC center's identity by assuming that only that center has access to its private key. The center signs the aircraft's certificate information including the original timestamp+1. The aircraft can decrypt this with the center's public key and be sure of the center's authenticity. However, the success of this requirement relies on the safety of each ATC's private key along with a relatively low clock skew between the aircraft and ATC. This risk is discussed in more detail later in the paper.

3. *All aircraft shall confirm the identity of other aircraft they are receiving data from*

   After an aircraft is authenticated by the local ATC center is has a session certificate to accompany its FAA certificate. Each aircraft with an ATC certificate is assumed to be valid, unrevoked FAA certificate. With this assumption each aircraft can freely authenticate any other aircraft by completing the aircraft-to-aircraft mutual authentication protocol described in section 4.6.2. Just like the two requirements above, this requirement can only be met if the ATC center's private key is kept secret along with each aircraft's private key along with a low clock skew.

5.2 Integrity Protection

There are three requirements for integrity protection. This section lists them out and explicitly states how each one is met through the DPP design explained in Chapter 4.

1. *The receiver shall have complete confidence that the information in each message has not been manipulated in anyway*

   All messages broadcasted by aircraft include both a raw form of the message along with a digital signature as described in section 4.5. This signature is a digest of the message encrypted with the aircraft's private key. Any entity which receives these messages can perform the same message digest on the raw message. If the entity has access to the aircraft's certificate can know its public key and therefore decrypt the signature block to reveal the message digest. If the message digest in the signature matches the one performed on the raw message then the receiver can have complete confidence that the information in each message has not been manipulated.

2. *The receiver shall be able to immediately determine if the contents of each message has been manipulated.*

   If the message digest in the signature does not match the message digest created by the receiver, the receiver can know immediately if the contents of the message have been manipulated.

3. *The receiver shall be able to immediately determine if the contents of each message was sent by an authenticated source.*

   If the sender is authenticated the receiving aircraft has a valid public key for the sending aircraft. Each message includes a digital signature signed with the sender's private key. If this signature is checked for validity the receiver can be certain of its origin by assuming that the receiver has validated the sender's public key and the private key of the sender has not been compromised.

5.3 Attack Mitigation

Each of the attacks listed in the attack model in section 3.3 are mitigated through aspects of the DPP design. The following section explicitly states how each attack is

mitigated and what specific design considerations were made in order to achieve mitigation.

Replay Attack. A replay attack is when an old message is replayed in an attempt to fool an entity into thinking they are communicating with someone else [6]. As described in section 3.3, someone could collect broadcasted messages from an aircraft or ATC and replay them later to cause a number of unintended consequences. There are three replay attacks that need to be mitigated: 1) replay during ATC-to-aircraft mutual authentication, 2) replay during aircraft-to-aircraft authentication and 3) rebroadcast of an previous aircraft's message. Each of which is mitigated through the following design aspects.

ATC-to-Aircraft: Given that each aircraft in a given center is authenticated by the local ATC center, each aircraft completes the ATC-to-aircraft mutual authentication protocol described in section 4.6.1. In this protocol, the aircraft provides a timestamp to have ATC sign and return. This is a standard and successful technique in many authentication protocols to prevent replay attacks [6].

Aircraft-to-Aircraft: During the protocol described in section 4.6.2 each aircraft is required to encrypt a timestamp in each message along with a session certificate which has an expiration date. If the expiration date has passed then the replay attack would be foiled. However, if the expiration date has not passed then the timestamp could be checked to validate that the message has not been replayed. These mechanisms ensure that each time the protocol is completed replay attempts can be easily spotted.

Message Rebroadcast: This attack is mitigated through the timestamp in each broadcasted message and the integrity check mechanism. Without the ability for an attacker to manipulate the message to include a different time a replay attack would be easily foiled.

Modification Attack: All messages that are broadcasted by each aircraft is protected against modification because of the digital signature that is appended to each message.

This ensures that if any part of the message was modified the receiver will notice as soon as the integrity check is complete.

Man-in-the-Middle Attack: There are two man-in-the-middle attacks that need to be mitigated: 1) man-in-the-middle during ATC-to-aircraft mutual authentication and 2) man-in-the-middle during aircraft-to-aircraft authentication. Each of which is mitigated through the following design aspects.

> ATC-to-Aircraft: In order to prevent man-in-the-middle attacks steps were taken to avoid someone taking advantage of the specific messages sent between ATC and the aircraft. If someone were to listen to both messages sent between ATC and the aircraft they could gain no further knowledge about either of their respective secrets. They could also not pretend to be ATC or the aircraft during the protocol due to the required knowledge of private keys.
>
> Aircraft-to-Aircraft: The main concern with a man-in-the-middle attack between aircraft is the ability for another entity to maliciously trick one entity into authenticating them. However, this is not an issue for this design considering that all broadcasted messages include a signature. A falsely authenticated entity would not be able to produce these signatures without knowledge of the private key. Therefore a man-in-the-middle attack during aircraft-to-aircraft authentication is not a concern.

FAA Insider Attack: If the private key that the FAA uses to sign aircraft and ATC center's certificates is compromised then the integrity of all certificates and therefore all entity authentication and data integrity is compromised. This will require mitigation through secondary systems and source multilateration as discussed in the background section 2.2.

ATC Insider Attack: The proposed design has a few characteristics which help mitigate some of the risk associated with an ATC insider attack. For example, if an ATC center's private key is compromised and an attacker can create fraudulent session certificates and attempts to mutually authenticate with another aircraft, that aircraft has the power to

request the spoofed aircraft's original FAA certificate. If the aircraft fails to present one then the attack is foiled.

An Aircraft's Private Key is compromised: If an aircraft's private key is compromised then the ATC center might try to mutually authenticate with a spoofed aircraft. If the spoofed aircraft has a valid key then the authentication protocol will be completed without any issues. However, the local ATC should have received a flight plan and a notification from another ATC center about the aircraft's arrival, all through the secure FTI. This would almost certainly lead the local ATC center to assume that the aircraft is spoofed. Another method of mitigation, although not as secure, is the double checking of the aircraft's existence through the secondary radar system.

The CRL is compromised: If the master CRL is compromised then old certificates could potentially be used to attack the system. This could cause ATC or aircraft spoofing. Both of these are mitigated through processes described above.

Now that all requirements are met and all attacks mitigated the next is to look at how the system would perform if it were implemented. The next section describes the method for determining system performance and discusses the results of the analysis.

Chapter 6
Performance Analysis

This section details the performance analysis done to estimate the implementation cost of the DPP design. It specifies the overhead caused by the authentication protocols, adding digital signatures to messages and the latency expected from computation of encryption and decryption. There are a number of assumptions that need to be made regarding the computational power of avionics on board aircraft and the transponder technology each aircraft has. There also needs to be decisions on key length and specific crypto algorithms that will be employed. All these aspects are discussed in the following sections along with a summary of the results.

6.1 Aircraft Avionics

All crypto functions will be performed on board aircraft and at all ATC centers. Considering that ATC has access to powerful computers the bottleneck in performance is going to be onboard the aircraft. Therefore, the processing performance of the system is going to be determined by how quickly and efficiently the aircraft's onboard processor sign messages and verify other signatures. The bottleneck in message bandwidth is going to be determined by the availability of the SBSS along with the onboard transponder technology sending and receiving messages. Both the onboard processor and the available bandwidth are discussed in this section.

6.1.1 Onboard Processor

As stated in section 2.2 the FAA is implementing NextGen as described in the NGIP [7] [8]. NGIP Appendix A lists a number of avionics systems which provide capabilities necessary to achieve the benefits of NextGen. The electronic flight bag (EFB) is one of these systems which provide the aircraft with the ability to perform basic computations using modern processors [8]. Several general aviation aircraft are using

iPads as EFBs and it is safe to assume that similar devices will continue to be used on more aircraft in the future. Current iPad models come equipped with an A6X chip which has a 1.4 GHz processor [36] [37]. Considering that aircraft are mandated to have ADS-B equipage by 2020 it is safe to assume that many aircraft will have access to similar processing power available through their EFBs.

It is important to note that if the DPP design were to be implemented then the FAA and industry would most likely design a processor whose only job would be to perform encryption and decryption [38]. This would streamline the comprehensive testing and verification that all avionics go through before they are certified to be on an aircraft. However, considering the available performance specifications of processors that are currently onboard, i.e. an iPad EFB, it is safe to assume these systems could perform the crypto operations before the installation of crypto specific hardware. For purposes of this performance analysis a 1.4 GHz processor is assumed to be on board and available for message processing.

6.1.2 SBSS and Transponder Bandwidth

ADS-B utilizes two transponder technologies 1) 1090ES and 2) UAT. For purposes of this performance analysis access to UAT technology is assumed. UAT data transmission allows for larger messages sent per second due to the frequency that it's on [35][39]. The frequency also has more bandwidth available for more aircraft to send and receive messages with low probability of collisions and missed messages. Typical UAT avionics boxes have data rates of 1.04 megabits per second (Mbps) [40].

The available bandwidth for implementation of DPP will depend more on the entire system architecture and what the SBSS can handle. Given UAT message length and available bandwidth on the frequency that it transmits messages there are a set number of message start opportunities (MSOs) which dictate the maximum number of aircraft that can broadcast messages without the risk of message collision [35][41]. There are a total of 4,000 MSOs per second. SBSS ground stations broadcast much larger messages than aircraft, some over 450 bytes. Therefore the FAA assigned 752 MSO's to be reserved to ground stations which make up 32 times slots due to the length of each

message. The rest are assigned randomly to aircraft in the area [35]. However, the limit of the available number of MSO's is dictated by the length of each message. This requires the signature block to be as short as possible in order to prevent it from reducing the number of aircraft which can occupy a space without the risk of message collisions.

This short message length requirement will be directly affected by the key length of the crypto suite chosen. Signature block size increases directly with key length [6] [19]. Therefore a strong crypto algorithm suite needs to be chosen with the shortest key length possible. The next section discusses the crypto algorithm chosen for the performance analysis of the DPP algorithm along with an appropriate key length which will provide the strongest encryption with the shortest key length.

6.2 Chosen Crypto Algorithm Suite and Key Length

An important component to a robust cyber security design is strong crypto algorithms accompanied by appropriate key size. Crypto algorithm strength correlates directly with key length and the encryption method chosen. Key length also effects the time it takes to encrypt and decrypt messages. Therefore it is important to first pick a suit of crypto algorithms to use then pick a key length that fits with the level of security required by the system [6] [19] [35] [42].

6.2.1 Crypto Suite Performance

There are many crypto systems that provide asymmetric keys that could be utilized in the DPP design. The ones considered for use in the DPP design need to produce public and private keys so certificates can be created. Potential asymmetric crypto suites analyzed in this paper are RSA digital signature, digital signature algorithm (DSA), elliptic curve cryptography digital signature (ECC) (ECDSA), and NTRU. RSA, DSA and ECDSA are established algorithms which have available performance benchmarks [43] [44]. Figure 6-1 and Figure 6-2 illustrates these three algorithms ability to sign and verify 59 byte messages, respectively, using different processors with varying clock speeds [43]. One would assume that the cycles would stay constant per algorithm

regardless of speed. However, processors speed has been known to vary with instructions per cycle which can drastically affect overall performance [45].

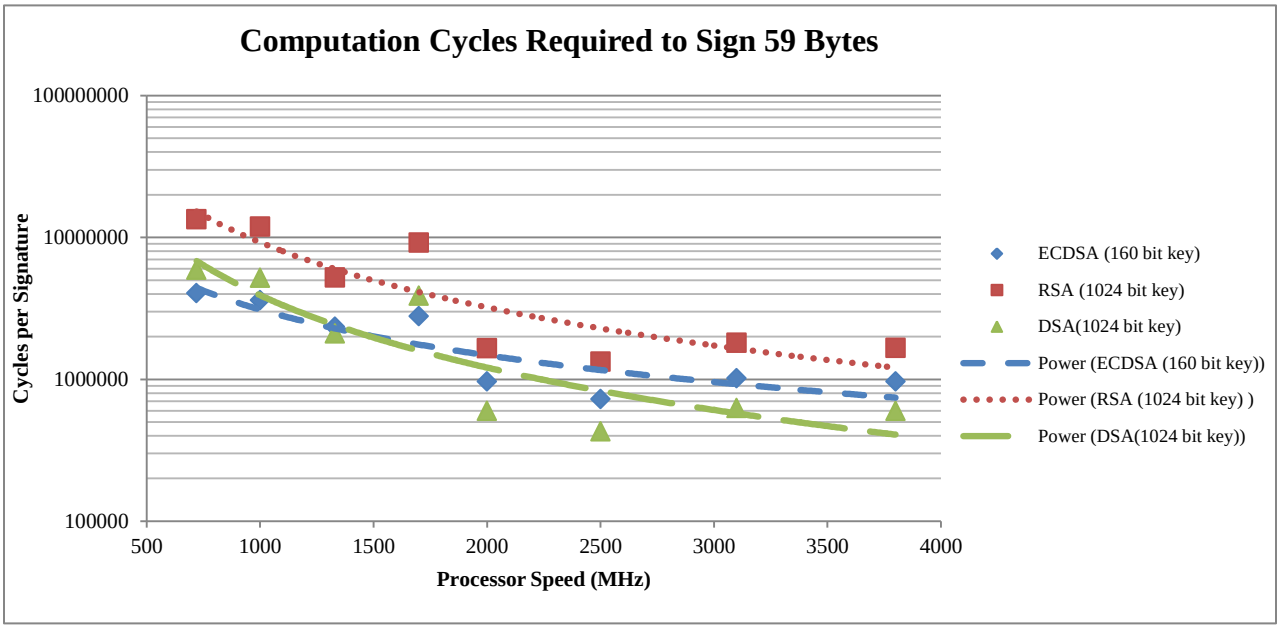

Figure 6-1. Computation Cycles Required to Sign 59 Bit Message **[43]**

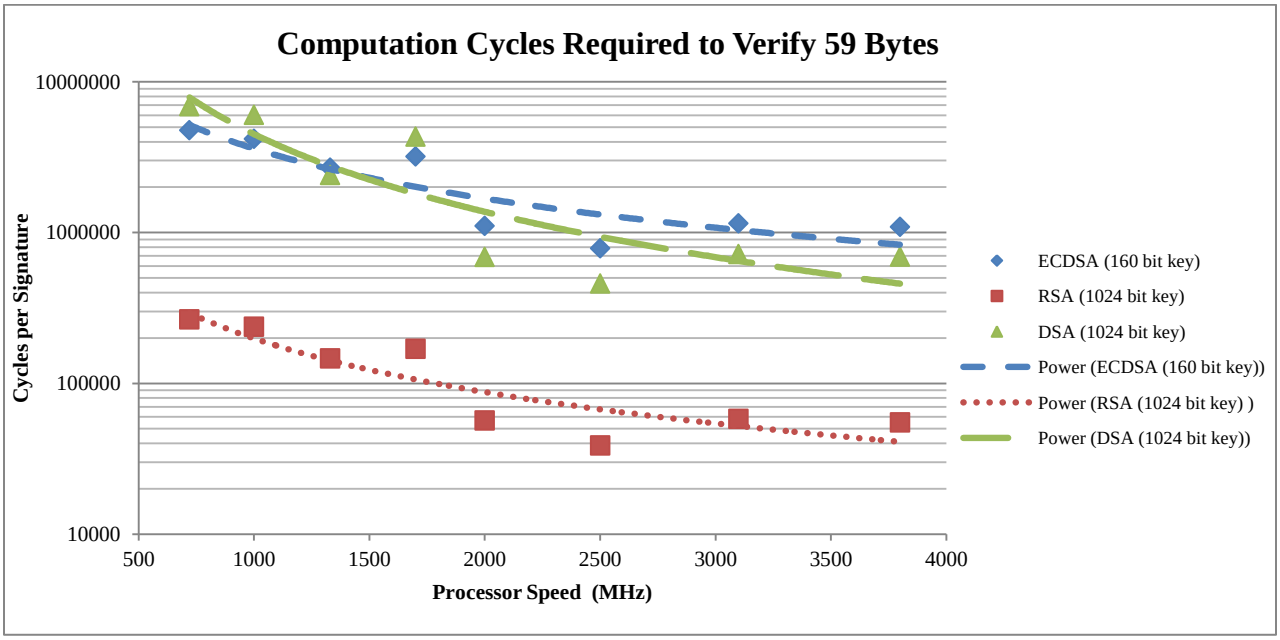

Figure 6-2. Computation Cycles Required to Verify 59 Bit Message **[43]**

These figures show that RSA is much more efficient when verifying messages. However, it is less efficient when signing messages. RSA would be a good fit if the ratio of verifying messages to signing messages were high. However, in the DPP design

aircraft-to-aircraft mutual authentication and verification only occurs between two aircraft at a time during the parallel arrival and departure procedures. This means each signed message will only get verified once. Also, considering the limited bandwidth of the SBSS it would be more advantageous to use an algorithm with shorter keys which, in turn, would produce shorter signature blocks. Considering ECDSA is just as secure with much shorter keys it makes it the obvious choice when compared to DSA and RSA. This is discussed in more detail in the next section.

The large exposure and increasing utilization of NTRU encryption technology makes it a viable candidate to be considered for the DPP algorithm [46] [47]. NTRU provides similar security to RSA and ECDSA with shorter processing time [46]. However, it requires even longer key lengths than RSA and DSA to provide the same security [46]. Despite the higher performance, larger signature blocks due to longer keys are not acceptable. Therefore NTRU is disqualified as a potential algorithm. The next section discusses RSA, DSA and ECC algorithms in terms of what key length makes most sense for the DPP crypto suite.

6.2.2 Key Length

Key length directly correlates with the strength crypto algorithms. This is typically measured in how long it takes to determine a key given a ciphertext and the associated plaintext. Table 6-1 below shows how symmetric, RSA/DSA/DH, and elliptic curve algorithm performance matches up with key length and time to break in terms of million instructions per second (MIPS) years.

Table 6-1. Comparisons of key lengths between crypto algorithms according to NIST **[42]**

Symmetric	RSA/DSA/DH	ECC	Time to break in MIPS years
80	1024	160	10^{12}
112	2048	224	10^{24}
128	3072	256	10^{28}
192	7680	384	10^{47}
256	15360	512	10^{66}

Note that ECC requires much shorter key lengths when compared to RSA/DSA/DH which would shorten the length needed for certificates. It has been proven that ECC is more efficient in terms of computational resources and bandwidth which makes it a perfect match for the DPP design [20] [42] [48]. Therefore, ECC crypto algorithms utilized through ECDSA signatures with a 160 bit key length are used for the performance analysis of the DPP design.

6.3 Mutual Authentication Performance

It is important to mention how each of the mutual authentication schemes perform given the available system infrastructure and the crypto system chosen. Each aircraft-to-ATC authentication protocol will only occur once when the ATC center assumes responsibility for the aircraft. Given that aircraft are under control of ATC centers for several minutes the performance of the authentication protocol will not be a concern to the performance of the overall system. This is similar to aircraft-to-aircraft mutual authentication where each aircraft will only need to authenticate another during a paired arrival or departure which will happen twice at a maximum during a flight. Given that mutual authentication protocols will not happen very often they will not be considered in as a limiting factor to the overall performance of the DPP design.

6.4 ECDSA Performance

The DPP design requires an efficient signature algorithm to complete the protocols described in Chapter 4. This is due to message signatures and verifications occurring often, possibly many times a minute. ECDSA is a robust and efficient method for digitally signing messages especially in environments where system resources are limited [20]. ECDSA was the first successful algorithm that utilized ECC crypto methods and has been accepted by the American National Standards Institute (ANSI), IEEE, National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) as a standard signature algorithm [48]. The performance of ECDSA must be specified in order to complete a comprehensive performance analysis of the entire system. This section discusses the performance of ECDSA applied to the DPP design in terms of processing speed and bandwidth consumption.

6.4.1 Processing Performance

The aircraft is the bottleneck in terms of computational power therefore the performance of the crypto algorithms onboard the aircraft need to be examined. These processes include the aircraft's ability to sign and verify every message that is sent and received, respectively. Assuming that ADS-B messages are broadcasted at 1Hz the performance of the signing and verifying algorithm needs to be relatively quick. Considering the message length, 32 bytes, key length 160 bits, and processor speed 1.4 GHz, these performance metrics can be calculated.

To determine the performance of the computation of a single signature or verification a benchmark for the performance of the ECDSA algorithm is required. These benchmarks can be found online and are broken out by algorithm, milliseconds per operation, and megacycles per operation for a particular processor. The benchmarks used to this paper are found at [43] and are illustrated in Figures 6-1 and 6-2. A high estimate for signature and verification performance is 3 and 4.5 megacycles, respectively. To determined time in seconds per operation the inverse of the processor speed is multiplied

by the cycles required per operation. Considering that the processor onboard each aircraft is assumed to be 1.4 GHz and all that processors resources would be devoted to DPP, a signature operation will take 2.14 milliseconds and a verification operation will take 3.21 milliseconds. These numbers will be used in the system wide evaluation performed later in this section.

6.4.2 Bandwidth Consumption

The major constraint on the implementation of the DPP design is the availability of bandwidth to handle the signature blocks on each broadcasted message. Considering the 160 bit key length for the ECDSA algorithm and assuming that signature blocks are twice the length of the associated key each message will be accompanied by a 40 byte signature. This will certainly reduce the number of available message slots available to aircraft broadcasting nearby. It will also reduce the total number of messages each aircraft can read in every second. However, the current SBSS should be able to handle the extra 40 bytes assuming 100% UAT equipage. When compared to messages broadcasted from the ground which are over 450 bytes, an additional 40 bytes to each ADS-B message will not clog the system. If there is a bandwidth issue, it can be mitigated by sending signatures along with the raw messages less often or reducing the ECC key length from 120 bits to 80 or even 40 bits.

This section discussed the individual performances of the application of ECDSA to DPP through examining the processing speed and bandwidth availability. Considering these performance statistics for the DPP design a higher level system wide evaluation can be performed.

6.5 System Wide Evaluation

The ECC algorithm suite, specifically ECDSA, along with a 160 bit key is chosen for the performance evaluation of the DPP design. Considering that no other aspect of the design cause significant performance issues, including mutual authentication protocols, the performance of ECDSA is the focus in determining the performance of the

entire DPP system. This is done through examining the implementation of the ECDSA algorithm limited by the available SBSS infrastructure and aircraft system resources. Evaluating each performance metric, both processor performance and bandwidth availability, it is found that the DPP algorithm would not cause any meaningful delay in either 1) the creation or processing of message signatures or 2) consume too much bandwidth when broadcasting of the signature block along with the original message. It is concluded that the DPP system could be successfully implemented. This conclusion along with other findings is discussed in the next chapter.

Chapter 7
Conclusions

The implementation of the DPP algorithm successfully fulfilled all requirements and mitigated many of the potential risks of aircraft-to-aircraft and aircraft-to-ATC communications. This section formalizes the conclusions that are drawn from the security and performance analysis of the design. There is also a brief section discussing possible applications of DPP and potential future work in the research area.

7.1 Thesis Findings

A thorough examination of the domains of ATC and cyber security revealed a potential issue with modern aircraft identification and monitoring practices along with the tools required to mitigate those issues. A formal definition of the problem and a search of similar potential solutions led the way to an understanding that the implementation of a strong PKI was appropriate. DPP is among the first proposed designs to handle the security vulnerabilities in aircraft-to-aircraft and aircraft-to-ATC data communications. The design solves the issue of aircraft identification through robust mutual authentication methods between aircraft and ATC. DPP implements modern ECC digital signature technology that allow aircraft to authenticate and integrity protect each message they broadcast. It also handles the difficult issue of certificate revocation through the novel implementation of a dual path key infrastructure and session certificates. An evaluation of DPP, constrained by current ATC infrastructure and onboard aircraft avionics and enabled through ECDSA, provided adequate proof that the system could be implemented successfully.

7.2 Future Work

The DPP design successfully accomplished all the requirements needed to successfully authenticate and integrity protect messages through contemporary cyber security methods. There is potential for other applications of the DPP design. This might also warrant slight modification of the design to accommodate different domains or constraints. The following section discusses potential DPP applications along with suggested expansions which might increase functionality or applicability.

7.2.1 DPP Potential Applications

One interesting potential application of the DPP design is using it to secure cockpit to controller data link communications (CPDLC). Similar to ADS-B, CPDLC allows controllers to send digital messages directly to the flight computer onboard an aircraft [49]. These messages typically include instructions to the aircraft regarding where to flight. Similar to ADS-B, CPDLC messages are sent in the open and are vulnerable to the same types of attacks. With a few slight modifications DPP has the potential to mitigate these attacks and secure CPDLC.

The DPP design gives a novel approach to handling certificate revocation by utilizing session certificates. It assumes that aircraft do not have a consistent connection to the current CRL. This is analogous to the VANET domain where there is a lot of research regarding efficient CRL dissemination. The DPP design could potentially provide a mechanism for vehicles inside of VANETs to authenticate certificates of other vehicles around them. One such application could replace the FAA with the DOT and ATC centers with road side units giving them the ability to sign and disseminate session certificates to vehicles in the area. However, the DPP design does not account for confidentiality.

7.2.2 Expansion of DPP Design

The DPP design could be expanded to allow for greater functionality. One potential area is the mutual authentication of aircraft. The DPP design only mutual

authenticates aircraft who wish to perform parallel arrivals and departures. This could be expanded to allow for multiple authentications. However, this will require another look at the crypto suit chosen, key length, and what the impacts on processing and bandwidth consumption may be.

There is also potential to link the FAA's application of the DPP design with international aviation PKIs. This can be done through a crosslink between the FAA's ability to sign certificates and another nation's CA [6]. There would need to be a secure connection between the international ATC centers and American centers so they could pass flight plan and certificate information between them. The nature of PKIs and the concept of chained certificate evaluation makes this a possible extension of the DPP design.

References

[1] M. S. Nolan, Fundementals of Air Traffic Control, Wadsworth, Inc, 1990.

[2] M. Mahmoud, N. Larrieu and A. Pirovano, "A performance-aware Public Key Infrastructure for next generation connected aircrafts," *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th,* vol., no., pp.3.C.3-1,3.C.3-16, 3-7 Oct. 20102010.

[3] V. Patel and T. McParland, "Public Key Infrastructure for Air Traffic Management Systems," *Digital Avionics Systems, 2001. DASC. 20th Conference,* vol.2, no., pp.7A5/1,7A5/7 vol.2, Oct 2001.

[4] K. Sampigethaya, R. Poovendran and L. Bushnell, "A Framework for Securing Future e-Enabled Aircraft," in *AIAA Infotech@Aerospace Conference*, 2009.

[5] K. Sampigethaya, R. Poovendran and L. Bushnell, "Security of Future eEnabled Aircraft Ad hoc Networks," in *The 26th Congress of ICAS and 8th AIAA ATIO*, 2008.

[6] C. Kaufman, R. Pearlman and M. Speciner, Network Security, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2002.

[7] FAA, "NextGen Implementation," FAA, 27 March 2013. [Online]. Available: http://www.faa.gov/nextgen/implementation/.

[8] FAA, "NextGen Implementation Plan," 2012. [Online]. Available: http://www.faa.gov/nextgen/implementation/media/NextGen_Implementation_Plan_2012.pdf.

[9] DOT, FAA, SBS Program Office, "Surveillance and Broadcast Services Description Document (SRT-047, Revision 01)," 2011. [Online]. Available: http://adsbforgeneralaviation.com/wp-content/uploads/2011/12/SBS-Description-Doc_SRT_47_rev01_20111024.pdf.

[10] DOT, FAA, SBS Program, "Interface Requirements Document (IRD)," 28 June 2010. [Online]. Available: http://faaco.faa.gov/attachments/NAS-1R-82530001_Interface_Requirements_Document_IRD_FAA_SBS_SDP_to_ATC_Automation_Service_Monitoring_User_Subsystems_V3_3_1_dated_062810_changes_accepted.doc.

[11] DOT, FAA, SBS Program, "ADS-B/ADS-R Critical Services Specification," 12 April 2007. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDkQFjAC&url=https%3A%2F%2Ffaaco.faa.gov%2Fattachments%2FSBSST_Critical_Services_Spec_20070412_RFO_Version_1_2.doc&ei=b1VgUaDDEdDw0QHn44H4CA&usg=AFQjCNGeGQpDRwQoJh_647_YCLDJ9Nn-Mw&bvm=bv.

[12] FAA, "Federal Telecommunications Infrastructure (FTI)," 29 June 2009. [Online].

Available: http://www.faa.gov/air_traffic/technology/fti/.

[13] J. H. Williams and T. L. Signore , "National Airspace System Security Cyber Architecture," 2011. [Online]. Available: http://www.mitre.org/work/tech_papers/2011/10_4169/10_4169.pdf.

[14] FAA, "En Route Automation Modernization (ERAM)," 16 November 2010. [Online]. Available: http://www.faa.gov/air_traffic/technology/eram/.

[15] Raytheon Company, "STARS and DASR Supporting GBSAA in the NAS," in *CNS/ATM Conference*, 2011.

[16] Indra Company, "Wide Area Multilateration System," 2009.

[17] S. Krishna and R. Poovendran, "Visualization & assessment of ADS-B security for green ATM," Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th, Oct. 2010.

[18] J. Krozel, Ph.D and D. Andrisani, II, Ph.D., "Independent ADS-B Verification and Validation," AIAA 5th ATIO and16th Lighter-Than-Air Sys Tech. & Balloon Systems Conferences, American Institute of Aeronautics and Astronautics., 2005.

[19] W. Trappe and L. C. Washington, Introduction to Cryptography, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2006.

[20] A. Iyer, A. Kherani, A. Rao and A. Karnik, "Secure V2V Communications: Performance Impact of Computational Overheads," *NFOCOM Workshops 2008, IEEE,* pp. 1,6, 13-18, April 2008.

[21] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in *Sigcom*, 2005.

[22] G. Samara, W. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANETS)," IEEE Wireless Communications, Vol 13, October 2006 ..

[23] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE,* vol., no., pp.1229,1237, 13-18 April 2008.

[24] J. Lee, H. Lee and G. Nam, "SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission," *Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on*, vol., no., pp.60,65, 26-28 April 2007.

[25] M. Raya, P. Papadimitratos and J.-P. Hubaux, "Securing Vehicular Communications," *Wireless Communications, IEEE,* vol.13, no.5, pp.8,15, October 2006.

[26] J. J. Haas, Y.-C. Hu and K. P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," *Selected Areas in Communications, IEEE Journal on,* vol.29, no.3, pp.595,604, March 2011.

[27] R. Sunnadkal, B. Soh and H. Phan, "A Four-Stage Design Approach Towards Securing a Vehicular Ad Hoc Networks Architecture," *Electronic Design, Test and Application, 2010. DELTA '10. Fifth IEEE International Symposium on,* vol., no., pp.177,182, 13-15 Jan. 2010.

[28] K. Karuppanan and K. Priya, "Secure privacy and distributed group authentication for VANET," *Recent Trends in Information Technology (ICRTIT), 2011*

International Conference on, vol., no., pp.301,306, 3-5 June 2011.

[29] G. Samara, W. A. Al-Salihy and R. Sures, "Efficient Certificate Management in VANET," *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, vol.3, no., pp.V3-750,V3-754, 21-24 May 2010.

[30] B. McKissick, "Wake Encounter Analysis for a Closely Spaced Parallel Runway Paired Approach Simulation," 9th AIAA Aviation Technology, Integration, andOperations Conference (ATIO), American Institute of Aeronautics and Astronautics., 2009.

[31] FAA, "Volume 3 General Technical Administration: Chapter 18 Operations Specifications," 12th March 2013. [Online]. Available: http://fsims.faa.gov/WDocs/8900.1/V03%20Tech%20Admin/Chapter%2018/03_018_003.htm.

[32] FAA, "Terminal Radar Approach Control Facilities (TRACON)," 1 February 2013. [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/ato/tracon/.

[33] FAA, "United States FAA Three Letter Location Decoder AAA to ZZV," [Online]. Available: http://www.faa.gov/air_traffic/publications/atpubs/LID/L_B.htm.

[34] RTCA, "DO-282B MOPS for UAT, ADS-B," RTCA, Inc, Washington D.C., 2009.

[35] NSA, "The Case for Elliptic Curve Cryptography," 15th January 2009. [Online].

[36] Apple Inc., "iPad Features," 2013. [Online]. Available: http://www.apple.com/ipad/features/.

[37] Wikipedia, "Apple A6X," 3 April 2013. [Online]. Available: http://en.wikipedia.org/wiki/Apple_A6X.

[38] Maxim Integrated, "Using ECDSA with the DeepCover Secure Microcontroller's (MAXQ1103) Modular Arithmetic Accelerator (MAA)," 17 June 2008. [Online]. Available: http://pdfserv.maximintegrated.com/en/an/AN4016.pdf.

[39] MITRE Corporation, "Universal Access Transceiver System Description," December 2000. [Online]. Available: https://docs.google.com/viewer?a=v&q=cache:DDYFa1vHjq8J:adsb.tc.faa.gov/WG5_Meetings/Meeting1/UAT-WP-1-03.pdf+&hl=en&gl=us&pid=bl&srcid=ADGEESibwrJFzsCb7MgkbSPe3OtCaf5jzz-pW06eF93LOrniH0rpbvJixculmF3_D10Gh1LqwaVbE-JGiEhwklhMggFzDq_y_XrEtYUpGZtrHgLarw7SUXv.

[40] Garmin, "GDL 90 UAT Data Link Sensor Installation Manual," 2006. [Online]. Available: https://www.google.com/search?q=GDL+90+UAT+Data+Link+Sensor+Installation+Manual&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a.

[41] MITRE Corporation, "System Description for the Universal Access Transceiver," November 2000. [Online]. Available: https://docs.google.com/viewer?a=v&q=cache:-nbiK0N1P9QJ:adsb.tc.faa.gov/WG5_Meetings/Meeting1/UAT-WP-1-09.pdf+&hl=en&gl=us&pid=bl&srcid=ADGEESicvGitVeGA9HYU6lmpOjqr8lj6fr

CK_UQ0JMFcE0owl56R4o5yh5R7KHKFJrb9gi-R-sG2mJfci4B5pWp-dvU1K6PhprrIyJXdDE91vfQB0tw4Tme.

[42] A. Khalique, K. Singh and S. Sood, "Implementation of Elliptic Curve Digital Signature Algorithm," *International Journal of Computer Applications (0975 - 8887),* vol. 2, no. 2, May 2010.

[43] eBACS, "ECRYPT Benchmarking of Cryptographic Systems," 6 March 2013. [Online]. Available: http://bench.cr.yp.to/.

[44] Crypto++, "5.6.0 Benchmarks," 31 March 2009. [Online]. Available: http://www.cryptopp.com/benchmarks.html.

[45] Wikipedia, "Instructions per cycle," 28 February 2013. [Online]. Available: http://en.wikipedia.org/wiki/Instructions_per_cycle.

[46] J. Hoffstein, J. Pipher and J. Silverman, "NSS: The NTRU Signature Scheme," *Advances in Cryptology - EUROCRYPT 2001,* vol. XII, p. 545, 2001.

[47] Tim Buktu, "NTRU Quantum-resistant cryptography," 2011. [Online]. Available: http://tbuktu.github.io/ntru/.

[48] G. Nabil, K. Naziha, F. Lamia and K. Lotfi, "Hardware implementation of Elliptic Curve Digital Signature Algorithm (ECDSA) on Koblitz Curves," Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on , vol., no., pp.1,6, 18-20 July 2012.

[49] H. Junru, "The improved elliptic curve digital signature algorithm," *Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on,* vol.1, no., pp.257,259, 12-14 Aug. 2011.

[50] Wikipedia, "Controller–pilot data link communications," 16 March 2013. [Online]. Available: http://en.wikipedia.org/wiki/Controller%E2%80%93pilot_data_link_communications.