Secure Operation, Control and Maintenance of Future E-enabled Airplanes

Krishna Sampigethaya*, Radha Poovendran*, and Linda Bushnell†
*Network Security Lab (NSL), EE Department, University of Washington, Seattle, WA 98195, USA
†Networked Control Systems Lab, EE Department, University of Washington, Seattle, WA 98195, USA

***Abstract*—Commercial aviation is at the threshold of the era of the *e-enabled airplane*, brought about by the convergence of rapidly expanding world-wide data communication infrastructures, network-centric information processing and commoditized lightweight computational hardware. With advanced avionics, processing and wireless communication capabilities, the e-enabled airplane can revolutionize the current air transportation system. However, the use of unregulated information technology and wireless technologies introduce vulnerabilities that can be exploited to provide unauthorized access to the onboard aviation information systems and impede their operation. The emerging security threats are not covered by current aviation guidance and regulations hence, remain to be addressed. This paper presents a comprehensive survey of security of the e-enabled airplane with applications such as electronic distribution of loadable software and data, as well as future directions such as wireless health monitoring, networked control, and airborne ad hoc networks.**

***Index Terms*—e-enabled airplane, loadable software, safety, security, health management, traffic control, ad hoc network**

I. Introduction

A. Overview

Over the last century, aviation has evolved to become a driving force for the global economy. In the year 2006, air transportation produced an estimated 3.5 trillion dollars, nearly 8% of the world gross domestic income [1]. However, air traffic has overwhelmingly increased over the decades, with number of passengers and amount of cargo transported on world-wide routes reaching an unprecedented 4.4 billion and 85.6 million tons, respectively, in 2006 [2]. Crowded skies combined with factors such as changing business models, terrorist threats, environmental concerns and passenger needs, test the current capacity and capabilities of air transportation systems. Consequently, today the aerospace industry is witnessing a revolutionary trend in commercial aviation, seeking technological and process innovations in aircraft design, manufacturing, operation, maintenance, and traffic management.

Large-scale initiatives are underway to assuredly integrate new aviation technologies into the civil airspace in the next two decades, with an expected three-fold increase in airspace capacity. In the USA, the Federal Aviation Administration (FAA) is collaborating with other government agencies, industry and academia to modernize the current National Airspace System to the Next Generation Air Transportation System [3]. Another similar initiative is the Advisory Council for Aeronautics Research in Europe [4].

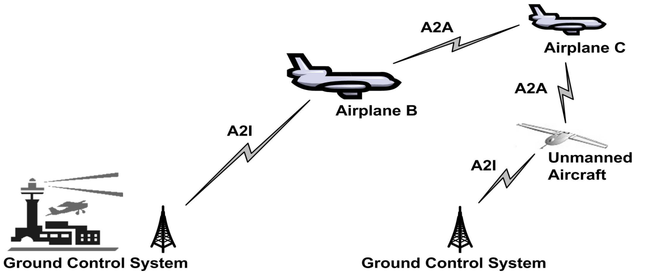

Fig. 1. Illustration of a future air transportation system with e-enabled airplanes, aircraft-to-ground (A2I) & aircraft-to-aircraft communications (A2A).

A recent vision in commercial aviation is the *e-enabled airplane*, i.e., an aircraft that can participate as an intelligent node in a global information network [5]. The e-enabled airplane is envisioned to possess advanced avionics highly integrated with wireless commercial technologies for automated functionalities, e.g., global positioning system for navigation [6], wireless sensors and Radio Frequency Identification (RFID) tags for maintenance [7], [8]. Wireless access points in the *in-aircraft network* will facilitate communications between onboard systems as well as communications with off-board infrastructure of air traffic control or airlines (*aircraft-to-infrastructure communications or A2I*) and another aircraft (*aircraft-to-aircraft communications or A2A*); see Fig. 1. Off-the-shelf and wireless solutions can substantially reduce onboard equipment maintenance overhead as well as system weight [5], [9], [7]. This fact and achievable enhancements in information delivery, availability, usage and management, make the e-enabled airplane a promising, cost-effective basis for improvements in flight safety, schedule predictability, maintenance and operational efficiencies, and other areas.

Latest developments strongly support the envisioned future of the e-enabled airplane. For instance, next-generation commercial airplanes have wireless access points for receiving loadable software [10], [11] and passive RFID tags for storing maintenance data [8], [16]. Other examples in commercial aviation include the introduction of 1090 MHz Extended Squitter data links for A2A/A2I [26] and broadband networked commercial unmanned aircraft systems [12].

However, due to the high-level of integration with off-the-shelf and wireless technologies, the e-enabled airplane information systems are not completely regulated nor isolated from external network access. New vulnerabilities are introduced that may open access to onboard systems and impede their operation, creating safety and airline business concerns.

Corresponding author: R. Poovendran (e-mail: rp3@u.washington.edu).

TABLE I

MOST RELEVANT STANDARDS FOR THE E-ENABLED AIRPLANE SECURITY. EDS - ELECTRONIC DISTRIBUTION OF SOFTWARE; AHM - AIRPLANE HEALTH MANAGEMENT; ATC - AIR TRAFFIC CONTROL; ADS-B - AUTOMATED DEPENDENT SURVEILLANCE BROADCAST

Application	Standard	Description
In-aircraft	[29]	Use of ethernet for in-aircraft networking
	[28]	In-aircraft network security guidelines for airlines
	[30]	Use of personal wireless devices onboard
EDS	[13]	Airplane software certification
	[19]	Signed crate format for secure EDS
AHM	[31]	Use of passive radio frequency identification tags onboard with passwords
ATC	[26]	ADS-B standards & applications for traffic beacons

Current guidance for airplane airworthiness from aviation regulatory agencies, e.g., [13], do not cover emerging security threats to the e-enabled airplane [14], [15], [16], [10]. Therefore, to ensure a safe, secure, reliable and efficient air transportation system with high capacity, security of the e-enabled airplane must be addressed. An important step towards streamlining this effort is to develop a unified framework for identification of security properties that the e-enabled airplane and its applications must satisfy, and for evaluation of candidate solutions. This paper provides such a framework, focusing on three representative applications for the operation, maintenance and control of the e-enabled airplane.

B. E-enabled Airplane Applications

Electronic Distribution of Software (EDS) [17], [10], [18]: Distribution of software for airplane systems has been via physical distribution of storage media (e.g., floppy/compact discs) and signed documents over bonded carriers. However, compared to this legacy FAA-approved process, the electronic distribution of software has advantages such as reduction of system weight from onboard storage media. The EDS[1] allows ground servers to deliver software and download data over A2I links from the e-enabled airplane. Aeronautical Radio Inc. is defining standards to secure the EDS for commercial airplanes [19], and industrial implementations are ongoing at Boeing and Airbus [11], [20]. Section V overviews the major security concerns with the EDS.

Air Health Management (AHM) [20], [9], [21]: A major goal of AHM is to improve maintenance overhead and lifetime of aircraft. In the e-enabled airplane, wireless sensors and RFID can meet this goal by offering a cost-effective means for continuously monitoring the health of structures and systems. Such a wireless-enabled AHM can provide timely feedback to an onboard computer via in-aircraft communications or to off-board units via A2I, enabling a paradigm shift in commercial aircraft maintenance from the fixed-interval scheduled process to an automated, real-time and proactive process [22]. Section VI discusses security of a wireless-enabled AHM.

Air Traffic Control (ATC) [23], [24], [25]: Recent events have highlighted the inefficiencies and lack of fault tolerance of current ATC due to a highly centralized architecture [23]. The e-enabled airplane presents several opportunities to decentralize ATC and share traffic control tasks, such as navigation and aircraft safe separation, with the ground controllers [23]. A recent example is the Automated Dependent Surveillance Broadcast initiative (ADS-B) [26] which can allow the e-enabled airplane to broadcast periodically (every second [24]) its identity and accurate location information to ground controllers (over A2I) as well as other airplanes (over A2A) for enhanced traffic surveillance and situational awareness [48]. Section VII reviews the security of a A2A/A2I-enabled ATC.

C. E-enabled Airplane Security Standards & Research

Table I presents some security standards for the e-enabled airplane. An ethernet-based architecture that protects flight-critical in-aircraft network systems from unauthorized access is in [29]. In [28], this architecture is improved with security mechanisms meeting airline constraints.

A well-established guidance for development of loadable software by onboard equipment suppliers is in [13], defining software safety-criticality levels based on impact of failure on flight safety, i.e., level A to level E with reducing criticality and development effort. Moreover, a data format for secure distribution of loadable software via EDS is in [19]. Recently safety implications from onboard use of personal devices, e.g., cellular devices and active RFID tags, is studied in [30]. Further, requirements for safe use of passive RFID tags on airplanes are identified in [31], e.g., use of password-based mechanisms for protecting tag data. Furthermore, ATC tasks based on the ADS-B are presented in [32].

Research efforts have also begun, focusing on issues not addressed by the above standards. In [5], [27], [20], [28], security mechanisms that can strengthen the in-aircraft network architecture are evaluated. In [17], [10], a security framework to analyze a generic EDS system is proposed. Further, in [7], [21], secure integration of wireless sensors and RFID in AHM is studied. Furthermore, in [18] potential impact of security solutions on onboard information systems is discussed.

In this paper, we provide an extensive survey of fertile research areas related to the e-enabled airplane, presenting state-of-the-art and identifying several open problems.

D. Paper Outline

Section II describes the overall system for the e-enabled airplane. Section III provides primitives and solutions to secure this system. Section IV–VII detail concerns due to vulnerabilities in the in-aircraft network, a generic EDS system, a wireless-enabled AHM and an e-enabled air traffic control, respectively. Section VIII discusses the e-enabled airplane security challenges. Section IX concludes the paper.

[1] Abbreviations used in the paper are in the Appendix.

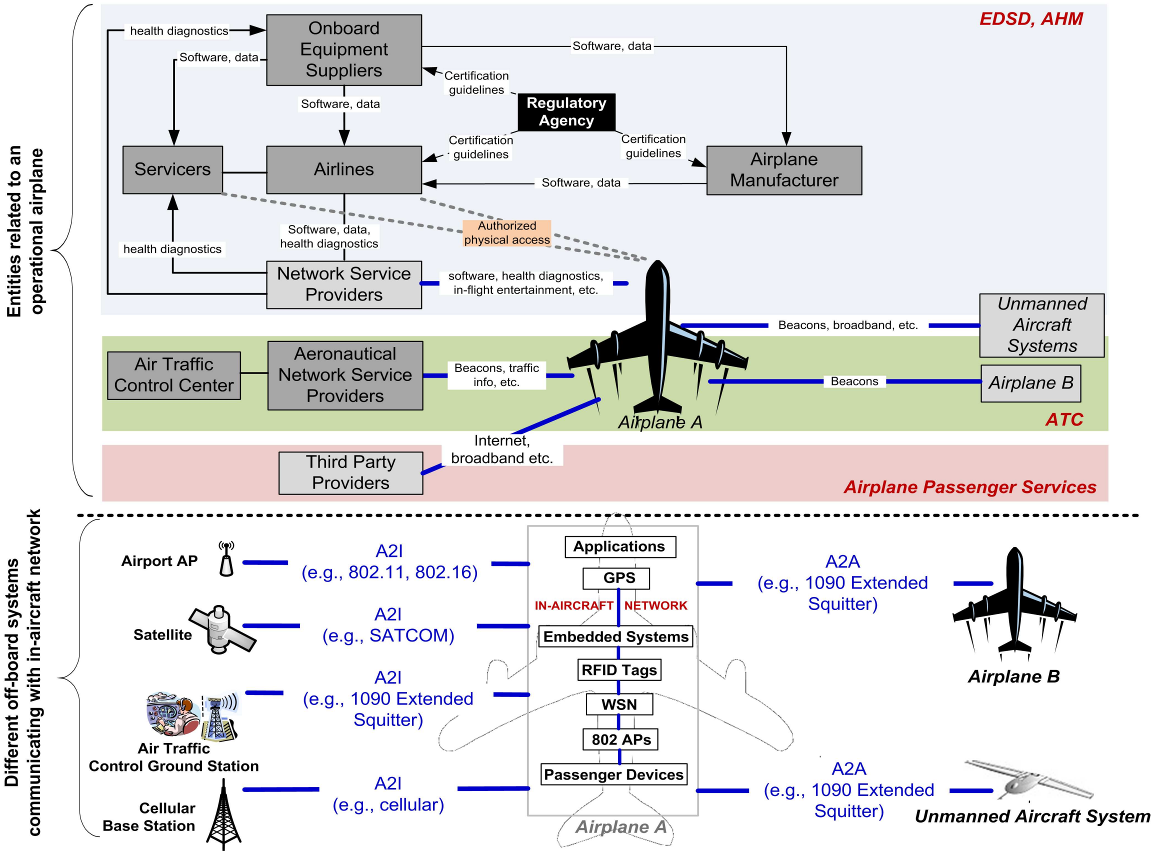
EDSD, AHM
Entities related to an operational airplane
health diagnostics
Onboard Equipment Suppliers
Software, data
Software, data
Certification guidelines
Regulatory Agency
Software, data
Certification guidelines
Certification guidelines
Servicers
Airlines
Airplane Manufacturer
Software, data
Authorized physical access
health diagnostics
Software, data, health diagnostics
Network Service Providers
software, health diagnostics, in-flight entertainment, etc.
Unmanned Aircraft Systems
Beacons, broadband, etc.
Air Traffic Control Center
Aeronautical Network Service Providers
Beacons, traffic info, etc.
Beacons
Airplane B
Airplane A
ATC
Internet, broadband etc.
Third Party Providers
Airplane Passenger Services
Different off-board systems communicating with in-aircraft network
Airport AP
A2I (e.g., 802.11, 802.16)
Satellite
A2I (e.g., SATCOM)
A2I (e.g., 1090 Extended Squitter)
Air Traffic Control Ground Station
Cellular Base Station
A2I (e.g., cellular)
Applications
GPS
IN-AIRCRAFT NETWORK
Embedded Systems
RFID Tags
WSN
802 APs
Passenger Devices
Airplane A
A2A (e.g., 1090 Extended Squitter)
Airplane B
A2A (e.g., 1090 Extended Squitter)
Unmanned Aircraft System

Fig. 2. An abstract model of the airplane information assets distribution system (AIADS) model in which the e-enabled airplane is operating. Dark grey boxes indicate trusted entities, and light grey boxes indicate untrusted entities. Blue (thick) lines represent A2A or A2I or in-aircraft network communications.

II. System Model of the E-enabled Airplane

Fig. 2 illustrates the considered system model called Airplane Information Assets Distribution System (AIADS). The AIADS distributes the e-enabled airplane *information assets*, i.e., information which is valuable for safe, reliable and profitable operation of the airplane. Based on the three representative applications, the information assets include loadable software (e.g., navigation databases, electronic flight bag, weather reports), health data (e.g., wireless sensor and tag data, diagnostics), and traffic control data (e.g., traffic beacons).

The top half of Fig. 2 shows that the e-enabled airplane has multiple entities communicating with it for each application, including: manufacturer, equipment suppliers, airlines, aeronautical and other network service providers, servicers (for maintenance), ATC centers, regulatory agencies (e.g., FAA), and other airplanes. The primary role of a regulatory agency is to certify the aircraft model and ensure compliance of entities with well-established safety guidance, e.g., Part 25 airplane generic configuration for the manufacturer [28], Part 121 airplane operational readiness for the airlines [28] and onboard software development practices for the suppliers [13].

Fig. 2 shows the flow of information assets. The responsibility of the AIADS for an information asset begins when the asset leaves its producer until the asset reaches its destination. The path between the producer and the destination is referred to herein as the *end-to-end path*. Each of the links in this path must fulfill the security objectives given later in Section III-B.

The lower part of Fig. 2 illustrates the integration of avionics with wireless technologies such as the global positioning system, sensors, passive tags, and 802.11 access points, in the in-aircraft network. A2I links with the airline infrastructure can be via a broadband satellite when the airplane is in-the-air [5] or a 802.11 link when on-the-ground [20]. Communications with the ATC ground stations is via aeronautical protocols [5] over satellite or terrestrial radio links. ADS-B provides an additional Mode S radio link with the ATC centers and also enables A2A links between neighboring airplanes. Currently, ADS-B based on 1090 MHz Extended Squitter link provides a narrow bandwidth communication range of 40 to 90 nautical miles [24]. We anticipate advances in wireless, such as 802.16, will provide long-range broadband connectivity. Further, it can be expected that passengers will soon access services from third parties using cellular/broadband links [30].

A. System and Trust Assumptions

Processes at each entity in the AIADS are assumed to be operating as designed and expected. In particular, the AIADS is assumed to be administered appropriately, e.g., proper assignment and management of access privileges at each entity, proper management and protection of passwords, cryptographic and security quantities. Each supplier is accountable to produce safety-assured loadable software [13]. Additionally, we assume that airlines manage software configuration of their fleet reliably and correctly; including the

TABLE II

COVERAGE OF THREATS TO AIADS ASSETS BY THE PROPOSED SECURITY REQUIREMENTS AND SOLUTION MECHANISMS. $\surd$ – SATISFIED; C – PARTIALLY SATISFIED; $\times$ – NOT SATISFIED.

Requirement/Threat	Asset Corruption	Asset Sensitivity	Asset Unavailability	Late Detection	False Alarm	Repudiation	**Solution Mechanisms**
Integrity	C	×	×	×	×	×	Digital signature
Authenticity	C	×	×	×	×	C	Digital certificate
Authorization	C	×	×	×	×	×	Digital certificate, RBAC
Confidentiality	×	$\surd$	×	×	×	×	Public key encryption, Symmetric key encryption
Correct & Early Detection	×	×	×	C	C	×	Signature check at each receiver on end-to-end path
Availability	×	×	$\surd$	×	×	×	Redundancy storage and bandwidth; Fallback to legacy mechanisms, etc.
Traceability	C	×	×	×	×	$\surd$	Tamper-proof logs, timestamps
Non-repudiation	×	×	×	×	×	$\surd$	Logging authorized actions

list of software/updates and latest software versions for each airplane model, and that airplanes can produce a configuration report accurately after receiving loadable software. The ATC and aeronautical service providers are trusted with traffic management tasks in the airspace. The providers of A2I links shared by multiple users, however, may not be considered responsible for airplane operation. Nevertheless, networks are assumed robust against well-known denial of service attacks.

B. Adversary Model Considered

Today, one must assume that terrorists as well as criminals pursuing economic damage are highly capable of employing advanced technologies for attacks on the e-enabled airplane. Therefore, we consider that the objective of an adversary is to lower the airplane safety margins (e.g., terrorist motivation) and/or to induce safety concerns and disturb airline business (e.g., motivation of sophisticated hackers or criminal organizations). We assume that the adversary is capable of external attacks – passive analysis or active manipulation of network traffic, and node impersonation – and internal (insider) attacks.

For simplifying exposition, we limit adversarial attacks to be only over data networks in the AIADS. Further, we note that insider attacks on the e-enabled airplane can be deterred by enforcing legal regulations and sufficiently safeguarded against with physical, logical and organizational inhibitors, checks and control. However, we consider insider threats for depth and completeness of our security analysis, and present solutions can enhance the level of protection to onboard systems.

In what follows, we propose our framework for securing the e-enabled airplane.

III. SECURING THE AIADS

We first identify the major threats to the AIADS assets.

A. Security Threats

1) Asset Corruption: The adversary may attempt to alter, insert or delete assets at any point along the end-to-end path between airplane and the source or destination of the asset to present threats to airplane safety or airline business. For example, some of the onboard systems contain safety-critical loadable software assessed to be at level A-C of [13], e.g., flight control computer, or business-critical loadable software assessed to be at levels D and E of [13], e.g., cabin light and in-flight entertainment systems. Malfunction of software in these systems can significantly degrade airplane airworthiness and/or create unwarranted flight delays/costs as well as visible disruptions in the operation of onboard systems, e.g., cabin light flickering. Other examples for critical assets of the e-enabled airplane include health diagnostics which may be manipulated to hide timely detections, and traffic beacons which may be corrupted to engineer mid-air collisions.

The adversary can also attack the AIADS for personal gain or for inducing unwarranted safety concerns that cause flight delays, cancellations and/or create passenger anxiety during flight, presenting additional threats to airline business.

2) False Alarm: Some assets can be corrupted to cause economic damage from misleading alarms. For example, the adversary can attempt to alter the software configuration report from the airplane to create mismatches between actual and intended configurations. Similarly, health diagnostics and traffic beacons may be manipulated.

3) Late Detection: Assets can be intentionally corrupted so that their detection is late enough for the airplane to be put out of service. For example, when corruption is detected in software received at the airplane or in health diagnostics distributed to the ground systems.

4) Asset Sensitivity: Some assets may provide leverage to the adversary for sidechannel attacks (e.g., fuel level data) or may be considered to be intellectual property with business value (e.g., RFID tag data).

5) Asset Unavailability: Assets can be made inaccessible, e.g., by jamming networks to disrupt airplane applications.

6) Repudiation: Any entity in the AIADS could deny having performed security-relevant actions on assets.

B. Basic Security Requirements

The AIADS needs to meet the following requirements to protect distributed assets from the above threats.

1) Integrity: For preventing any corruption of distributed assets by the adversary, the identity and content of the asset received at the destination must be verified to be the same as at the distribution source.

TABLE III

AIADS CONSTRAINTS ON THE E-ENABLED AIRPLANE AND IMPLICATIONS FOR ITS APPLICATIONS AND SECURITY.

Constraint	**Implications for e-enabled Applications and Security**
Airplane lifetime	Long-term security solutions
Stages of airplane operation	Fixed performance time constraints
Regulatory Requirements	Can be incorporated with existing well-defined regulations
Airline Business Requirements	Performance overhead cost and time constraints
Airplane Legacy Systems and Processes	Need for compatibility with existing onboard systems; Can use legacy mechanism as backup
Global Scale of Traversed Path	Standardization/adaptability and scalability Ability to work offline

2) Source Authenticity: For preventing injection of corrupted assets by unauthorized entities, the identity of each entity performing an action of any asset must be verifiable.

3) Authorization: The verifiable identity of each entity accessing any asset, must be checked to possess the appropriate permission and privilege.

4) Confidentiality: Unauthorized access to sensitive assets must be prevented to protect intellectual property and prevent any future attacks.

5) Correct and Early Detection: In order to prevent unwarranted flight delays and costs, any manipulation of an asset must be detected as soon as possible, while also eliminating or reducing false alarms.

6) Availability: Each asset must be available on time to meet regulatory and airline needs (discussed in next section).

7) Traceability: All actions performed on each asset must be logged in a format and for a time period that can satisfy both regulatory and airline needs.

8) Non-repudiation: In order to support forensics, such as after occurrence of safety hazards, the traceability of actions on each asset must be undeniably associated with at least one authorized entity.

Table II shows which threats can be mitigated by the security requirements. We now present some of the major constraints of the AIADS system that can impact these requirements and potential defense mechanisms.

C. Relevant System Constraints

1) Lifetime of the Airplane: Average lifetime of a typical commercial plane, and hence of its assets, is in the order of several decades. Time-dependent security requirements for the airplane assets, such as non-repudiation, must take this constraint into account. Further, the constraint imposes the need for long-term security solutions.

2) Stages of Airplane Operation: The different phases of flight can be categorized into three operational stages: on-the-ground, takeoff/landing, and in-flight. The time period of each operational stage of the airplane is fixed. Applications and their security mechanisms are therefore expected to function within these time constraints.

3) Regulatory Requirements: Additionally, certain mandatory guidelines from regulatory agency must be met for the airplane to be considered airworthy and ready for flight.

4) Airline Business Requirements: The airline fleet operation and maintenance costs must be reduced. Therefore, any security solution must minimize its overhead.

5) Legacy Systems and Processes: In order to obtain return-of-investment from existing onboard systems and processes, new technologies must be compatible with legacy systems and processes in commercial aviation [20].

6) Global Scale of Traversed Path: An airplane may traverse multiple airports during its end-to-end flight, with possible lack of network connectivity at any traversed airport or during flight. At each airport, the airplane can encounter varying conditions such as in terms of protocol standards, security technologies, export restrictions [20], and multiple off-board systems (e.g., airport wireless access point and airline information systems) may communicate with the airplane. Security solutions therefore must be adaptable and scalable to ensure seamless air travel for the airplane.

As seen in Table III, any solution approach for securing the e-enabled airplane and applications, must take into account the above constraints.

D. A Solution Approach for AIADS

1) Use of Digital Signatures: Digital signatures constitute one the potential mechanisms to secure distributed assets in the AIADS. We note that the choice of using digital signatures, as opposed to other solutions such as keyed cryptographic hashes and virtual private networks, is made in order to additionally provide non-repudiation and source authenticity along with integrity across multiple AIADS entities. A generic signed asset from a source to a destination in the AIADS can be of the form:

$$asset, sign_{source}(h(asset), tstamp), cert_{source}$$

where $sign_x(.)$, K_x denote signature and public key, respectively, of an entity x. $h(.)$ is a one-way cryptographic hash and a, b denotes concatenation of two strings a and b. The digital certificate of a trusted Certificate Authority (CA) is of the form:

$$cert_{source} = sign_{CA}(source, K_{source}, CA, validity\_period).$$

Assuming the CA's public key is known, the destination can use $cert_{source}$ and $tstamp$ to verify the integrity and source authenticity of the received asset. Verifying signatures as soon as possible at each intermediate entity along the end-to-end path in AIADS can contribute to the *correct and early detection* of corrupted assets. Signatures in combination with audit logs are sufficient for achieving *non-repudiation* and *traceability*.

Later in Section VIII, we discuss the major challenges posed by the AIADS constraints when using digital signatures as a solution mechanism.

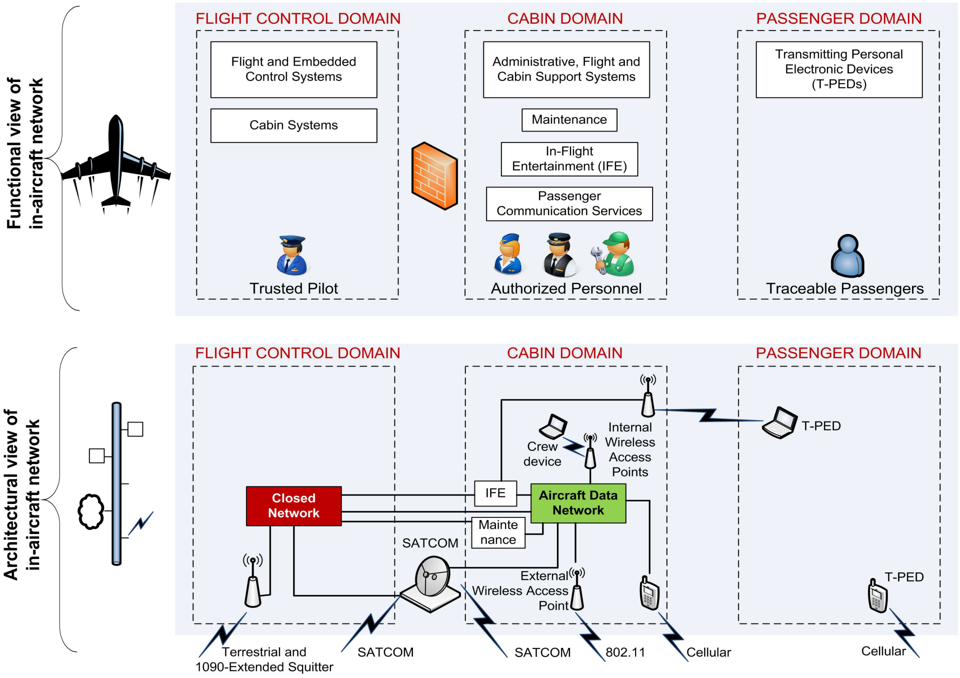
Functional view of in-aircraft network
FLIGHT CONTROL DOMAIN
Flight and Embedded Control Systems
Cabin Systems
Trusted Pilot
CABIN DOMAIN
Administrative, Flight and Cabin Support Systems
Maintenance
In-Flight Entertainment (IFE)
Passenger Communication Services
Authorized Personnel
PASSENGER DOMAIN
Transmitting Personal Electronic Devices (T-PEDs)
Traceable Passengers
Architectural view of in-aircraft network
FLIGHT CONTROL DOMAIN
CABIN DOMAIN
PASSENGER DOMAIN
Closed Network
IFE
Aircraft Data Network
Mainte nance
Crew device
Internal Wireless Access Points
T-PED
SATCOM
External Wireless Access Point
T-PED
Terrestrial and 1090-Extended Squitter
SATCOM
SATCOM
802.11
Cellular
Cellular

Fig. 3. An abstract model of the in-aircraft network architecture and domains, showing logical connections between components.

2) Additional Security Mechanisms: All security-relevant actions during asset distribution as well as actions related to the associated certificates, must be *authorized*, e.g., using role-based access control. Further, for *traceability*, all security-relevant actions, including unsuccessful attempts, must be timestamped and logged in tamper-proof storage. *Availability* for the AIADS systems, especially those supporting A2I applications, can be achieved with host and network protection mechanisms [5]. Further, the A2A and A2I data links can be secured via higher layer security mechanisms, such as IP security at network layer and Secure Socket Layer at transport layer; see [5] for a survey of potential mechanisms.

Any copyrighted or sensitive asset requiring *confidentiality* can be transferred over an encrypted channel, e.g., network layer encryption between airport access point and airplanes. Additionally, some communications in the AIADS may be subject to stringent delay and/or resource constraints. In such cases, symmetric key cryptography offers solutions, e.g., Secure Socket Layer, that are more efficient compared to those based on asymmetric key cryptography [5].

Table II shows the requirements and threats satisfied by the solution mechanisms given above. However, as seen in Table II, these mechanisms may not be sufficient to fully meet the security requirements. Vulnerabilities in the distribution of AIADS assets over the in-aircraft network as well as over A2I/A2A applications must be separately addressed.

IV. Securing the In-Aircraft Network

As illustrated in Fig. 3, based on [29] and [28], information systems on the in-aircraft network of the e-enabled airplane can be logically separated into three domains: *flight control, cabin and passenger* [28]. The flight control domain consists of avionics and control systems handling safety-critical onboard operations, navigation and surveillance. Failure of these systems has a direct impact on flight safety. On the other hand, the cabin domain systems mostly support only business critical onboard operations (e.g., cabin lights), maintenance (e.g., health monitoring) and passenger entertainment functions. The passenger domain consists of wireless-enabled personal electronics, such as laptops and cellular devices, that do not support any flight related function.

Attacks on the assets in the in-aircraft network can emerge from vulnerabilities in the passenger and cabin domain, e.g., malware based attacks and signal jamming attacks by the wireless devices carried onboard [29]. A solution approach is to secure all cross-domain communications at multiple layers by using sufficient physical, logical and organizational inhibitors, e.g., network firewalls, routers, switches and monitoring tools [5], [27], [28] and usage policies for wireless devices carried onboard. These measures along with other host based mechanisms (e.g., efficient filtering, redundant storage, tamper-proof logging of security-relevant actions) ensure that the flight control domain is operational and closed to passenger domain as well as protected against unauthorized access/passive eavesdropping from cabin domain [20]. Similarly, cabin domain is secured from passenger domain.

Overall, such an approach has the potential to protect AIADS assets distributed over in-aircraft communications. However, threats to these assets can emerge from vulnerabilities in the EDS, AHM and ATC applications of the e-enabled airplane. We cover these threats next.

V. Securing Airplane Loadable Software Assets

Apart from the well-established guidance in [13] to assure loadable software development at suppliers, in Section III we proposed the use of digital signatures for integrity and authenticity of loadable software distribution from suppliers to the e-enabled airplane via the EDS. The software is finally

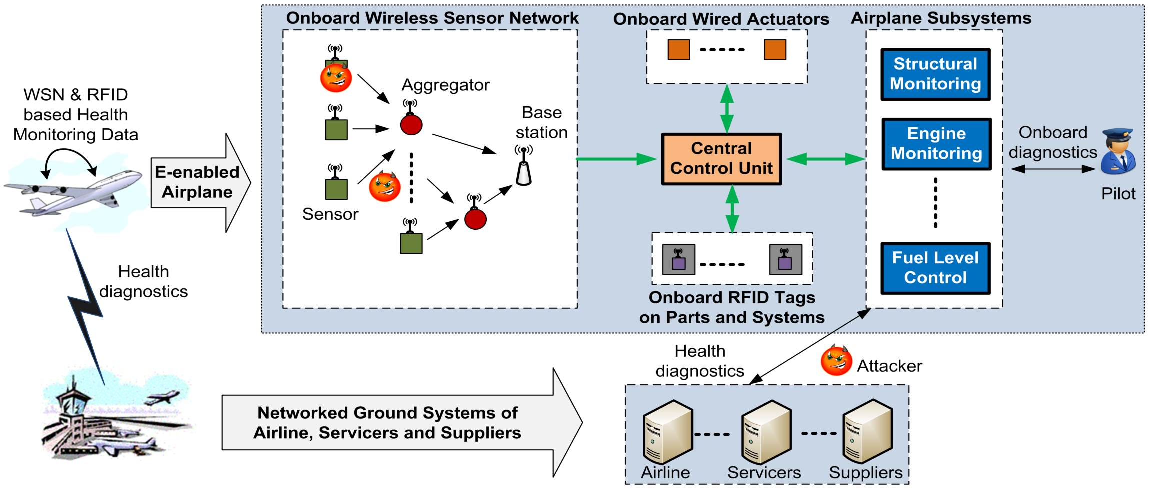

Fig. 4. Illustration of the AHM model considered, containing wireless sensors and RFID tags onboard to collect health data and enable automated and real-time health monitoring. The resulting health diagnostics can be distributed to ground systems for proactive aircraft maintenance.

uploaded into the onboard embedded systems by a dataload process. Regulatory agencies mandate that this dataload process is sufficiently protected and controlled. For example, loading is only performed at specified times, such as when the airplane is in maintenance mode, and by authorized personnel using authorized equipment. During the dataload process, additional checks are in place to detect corrupted software, including: *(i) Cyclic Redundancy Code check* by the embedded system for detecting accidental modifications of software, *(ii) onboard generated configuration report check* to verify that distributed software matches a configuration list at the airline, and *(iii) compatibility check* of the uploaded software with the destination hardware and software environments. However, the dataload process presents vulnerabilities that must be addressed by separate measures in the EDS.

A. Addressing Vulnerabilities in EDS

1) Use of Onboard Software and Hardware Redundancy: The adversary may alter or replace contents of the loadable software with non-arbitrary bit substitutions, making the corrupted software pass the error check during and loadable at the destination. Therefore, safety-critical software and hardware must incorporate redundancies, e.g., several code instances executing in parallel on different system platforms on the airplane, to tolerate and/or detect corrupted software. In order to effectively cripple a safety-critical function in the airplane, the representation of software must be modified at several positions. While this increases the adversary effort, it may restrict the desirable automation of onboard software maintenance.

2) Use of Metadata for Digital Signatures: Loadable software may be incompatible across different software versions and airplane models. The adversary can attempt to exploit this vulnerability and prevent or delay A2I distribution of signed software updates to an airplane as well as divert signed software intended for another airplane model, resulting in anomalies during the compatibility check. A mitigation approach is to include a metadata with the signed software:

$$asset, metadata, sign_{source}(h(asset), metadata, tstamp),$$
$$cert_{source}$$

where $metadata = ver\_num, intended\_dest$. The version number ver_num and the timestamp $tstamp$ ensure that outdated software is not accepted, assuming again that airlines manage the configurations of the airplanes. The intended destination $intended\_dest$ in the signed metadata ensures that diverted software is not accepted at incorrect destinations.

B. A Major Challenge in EDS

In order to integrate the EDS with well-defined guidelines for loadable software development and dataload process that ensure airworthiness, a standardized approach is needed to identify security requirements in a systematic way. Such an approach is proposed in [10], [17], where the Common Criteria methodology is used for security analysis of a generic EDS system. Emerging as a well-known standard for information system security, Common Criteria provides a framework to identify threats, derive security objectives, state security functions, and specify an evaluation assurance level [34].

Both the EDS and AHM, depend on digital signatures to protect data from the e-enabled airplane to the ground systems, i.e., software configuration report and health diagnostics, respectively. However, with the integration of wireless sensors and RFID tags in the AHM, the onboard collection of the data used in health diagnostics is vulnerable, as seen next.

VI. Securing Airplane Health Assets

We first describe the AHM model, and then discuss major vulnerabilities and their mitigation.

A. Wireless-Enabled AHM Model

Fig. 4 illustrates the AHM model considered in this paper. Passive RFID tags are attached to onboard systems and parts for storing their maintenance data. Smart sensors which possess a signal processing unit, memory and a wireless communication unit, are deployed on airplane structures and systems for health monitoring. These sensors may have heterogeneous capabilities (e.g., node transmission range) and modalities (e.g., vibration, temperature, pressure etc). Further, due to energy constraints, they form a wireless sensor network

(WSN) with multi-hop routes where each sensor communicates directly with one-hop neighbors, i.e., nodes in its radio range. To reduce the overwhelming volume of health data, we assume in-network data aggregation in the WSN [35].

The aggregator nodes forward data to a base station which provides this feedback to a central control unit. The feedback is finally sent to the intended airplane subsystems. The data collection in the WSN can be done periodically, or upon detection of an event by one or more sensors (e.g., abnormal increase in structural temperature) or on demand by the control unit (e.g., query to determine the fuel level). The airplane subsystems analyze the feedback received from sensors owned by them. The analysis can lead to execution of tasks at the subsystems, such as notifying the pilot or triggering some onboard actuator or initiating a downlink of diagnostics to the ground systems via A2I link. The authorized ground systems of airlines are also capable of initiating download of health data when their airplanes are on the ground and/or in flight.

We assume that the wireless sensors and RFID tags do not degrade under the harsh flight conditions, such as extreme hot/cold temperature and high vibrations. We also assume that sensors for assessing safety-critical parts are subject to physical checks when validating airplane airworthiness; additionally these sensors have a backup hard-wired connection to the control unit to enable cross checks for verifying consistency of the generated wireless readings. Nevertheless, use of wireless channels allows an adversary to perform remote attacks that can manipulate avionics operation in unexpected ways.

B. Use of Link Key Cryptography

Since we assume that sensors are energy-constrained, symmetric cryptography is more suited for providing integrity, authenticity and confidentiality of WSN communications, as opposed to asymmetric cryptography which is relatively computation and communication intensive. Further, in the WSN, solutions based on link layer cryptography, i.e., using a cryptographic key shared by two neighbors, are more suited, when compared to end-to-end solutions [36].

The link keys, however, need to be established by the WSN nodes upon deployment. Since the topology of the WSN is assumed to be pre-determined before deployment, the key establishment problem is simplified [37], [38]. A potential solution can be based on the tamper-resistant base station that shares a pre-distributed pairwise key with each sensor node before deployment. In such an approach, two neighboring sensor nodes can later establish their link keys via the base station. On the other hand, administration of keying material in the AHM is challenging as will be discussed later.

However, the use of cryptography alone is insufficient to address vulnerabilities in the WSN and RFID [36], [39], [44]. Threats from jamming and sidechannel attacks on the network protocols translates to the following primitives.

C. Addressing Vulnerabilities of WSN

1) Mitigation of Channel Jamming: The adversary can, for example, employ jamming attacks to block or delay safety-critical fault detections from propagating towards the base station. Therefore, channel jamming attacks must be detected as soon as possible and mitigated in the WSN. A potential solution is in [40], where a network node adjusts its transmission rate in order to contain jamming interference.

2) Secure Routing: The sensors in WSN need to route their readings timely and reliably even under attacks. The WSN routing protocol must be robust to jamming attacks that induce long and energy-inefficient routes. The routing protocol must also be robust to attacks based on misleading routing messages. For example, if geographic routing is used then by spoofing location information (e.g., wormhole attack [39]) a compromised node can modify routes at will.

3) Secure Location Verification: Sensor readings are only useful when associated with their physical locations [41]. For example, sensor data that represents a detected crack in the aircraft structure will be useless if it does not include a physical location for the crack. Further, network services, such as geographic routing, depend on node location information [41]. Hence, WSN nodes must be able to securely verify location claims of their neighbors to address attacks based on spoofed location data, e.g., the wormhole attack on geographic routing [42], [43]. Secure location verification also provides another level of source authentication using the position of a neighbor to validate data received from it.

At the same time, the location of some sensors that are used for safety-critical detections may be of interest to the adversary for launching sidechannel attacks. Consequently, the communications in the WSN must not reveal the location and type of such sensors to unauthorized entities.

4) Robustness to Sensor Capture: For insider attacks based on compromised sensors, tamper-proof sensor hardware offers a potential solution. However, since this solution is expensive and adds to avionics overhead, the design of WSN algorithms for the above primitives must be capable of tolerating compromise of a fraction of network nodes [38].

D. Addressing Vulnerabilities of RFID

Unlike the dynamic data observed by wireless sensors, the static nature of information stored in the passive RFID tags onboard the aircraft may imply a false sense of security. However, with the proposed onboard use of transmitting personal electronic devices including RFID tags in the passenger domain [30], potential threats emerge to the integrity, authenticity, confidentiality and availability of the passive RFID tag data [44]. Attacks including spoofing, unauthorized access and passive eavesdropping of the stored data can disrupt business of the data users, including the airline, servicers and suppliers. For example, a bogus tag with a spoofed identity can prevent an expired part from timely replacement. Therefore, security primitives such as robustness to tag impersonation, read access control and robustness to denial of service (e.g., the kill command) must be met by the RFID system [44].

E. Major Challenges in Wireless-Enabled AHM

Wireless sensors and RFID tags have unique properties compared to current avionics, yet they may be subject to similar high performance needs and operational processes existing

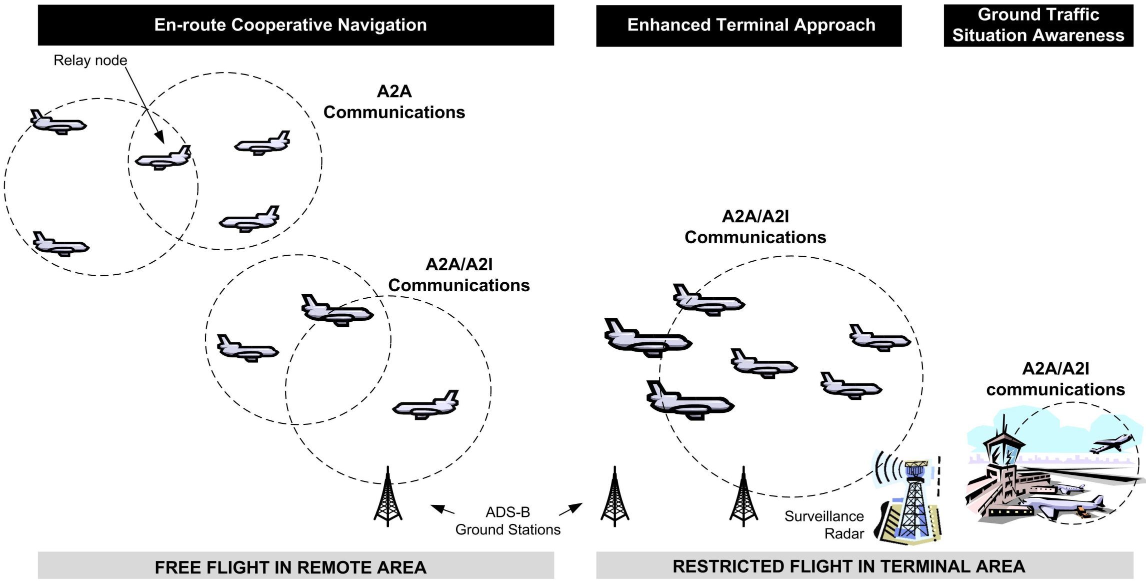
En-route Cooperative Navigation
Enhanced Terminal Approach
Ground Traffic Situation Awareness
Relay node
A2A Communications
A2A/A2I Communications
A2A/A2I Communications
A2A/A2I communications
ADS-B Ground Stations
Surveillance Radar
FREE FLIGHT IN REMOTE AREA
RESTRICTED FLIGHT IN TERMINAL AREA

Fig. 5. Illustration of considered ATC applications with e-enabled airplanes. Circles indicate a communicating group of nodes (aircraft and ground stations).

onboard. Consequently, a number of unprecedented challenges can be anticipated while adopting these technologies onboard.

1) Providing Power Efficient Solutions for WSN and RFID Tags: Wireless sensors and tags may be subject to a periodic maintenance as current avionics. Assuming the maintenance period can vary in the order of a few weeks to months, the wireless sensors and tags must be able to operate reliably within their energy constraints during this period. For conserving the battery power of the WSN nodes, a balanced combination of sensor processing and energy-efficient data aggregation algorithm is needed. Further, the WSN medium access algorithm employed must also be energy-efficient, e.g., by making nodes periodically enter sleep mode when not active [36]. Additionally, the solution design for the above primitives must incorporate this energy constraint, e.g., by designing energy-efficient secure broadcast routing [45].

2) Ensuring Low End-to-End Path Latency in WSN: Similar to other onboard systems whose response is time-critical, it is pivotal that all detected safety-critical faults are delivered in a timely manner by the WSN to the central control unit for real-time diagnosis by the airplane subsystems, and if needed to the ground systems for further analysis. Consequently, the WSN routing algorithms must be designed to be energy-efficient, but under a maximum end-to-end delay constraint.

3) Providing Traceability under Data Aggregation in WSN: As seen from Section III-B, traceability of authorized actions taken in the AIADS is inherently important. However, use of data aggregation obscures traceability of data in the WSN, reducing, in most cases, the ability to identify the source of the false or malicious fault detection data. The data aggregation algorithm employed in the WSN must address this tradeoff.

4) Accommodating WSN Membership Dynamics: Like other onboard systems, nodes in the WSN can be expected to be removed or replaced over time. Consequently, the key management scheme and policy must be capable of allowing node additions and deletions from the WSN, while also ensuring secure periodic key updates in the network.

5) Impact of Active RFID Tags on Airworthiness: In [16], the certified use of passive-only RFID tags onboard commercial airplanes is provided. However, due to safety concerns, the use of active RFID tags still remains to be studied and approved. One of the safety concerns include the potential for their electromagnetic interference with the operation of flight-critical avionics systems. Any future approval of the use of active RFID tags onboard would however provide a stepping stone for the use of the WSN enabled AHM.

The airplane together with the A2I networked ATC ground controllers and other A2A networked airplanes, becomes part of a large-scale decentralized control system that enables global traffic-relevant decisions (e.g., aircraft altitude control) at the ground as well as onboard controllers [23]. The security of this control system, specifically of its A2I and A2A communication networks, is considered next.

VII. Securing Airplane Traffic Assets

In this section, the ATC model considered is described, followed by the vulnerabilities that must be addressed.

A. E-enabled ATC Model

Each airplane periodically broadcasts (approximately every second) its state vector containing position, altitude, speed, time and other information [48]. These beacons can be utilized by the ground controllers and other airplanes. The enabled automated surveillance applications can be broadly classified as: A2I-Out and A2/A2A-In [48]. In the A2I-Out applications, the periodic beacons are utilized only by ground controllers for surveillance. In the A2I/A2A-In applications, the periodic beacons are also used by other airplanes to enhance pilot's situational awareness, and the ground controllers can communicate traffic and weather reports to the airplanes.

Fig. 5 illustrates some of the applications that use networking and other key enablers such as conflict resolution algorithms, to potentially optimize air travel with respect to time and cost (e.g., fuel expenses) [49]. Airplanes traversing remote areas can engage in *Free Flight*, i.e., each airplane can self-optimize by choosing its own route, altitude, speed, etc [23]. Further, the flow of air traffic in a typically congested terminal area can also be optimized, and ground delays at the gates, taxiways and runways can be significantly reduced [24]. Further, multi-hop communications in airborne networks can extend information reachability to airplanes in remote areas such as oceans or mountainous regions [24].

While world-wide deployment of enabling infrastructures, e.g., ADS-B [26], support the future of airborne ad hoc networks in commercial and general aviation, several networking and security challenges remain to be resolved. An abundance of literature, during the last decade, addresses the airborne ad hoc networking issues such as the design of transmission protocols and the impact of air traffic on the network topology (http://www.airborneinternet.org, [24], [25]), as well as the design of safety-critical airborne traffic operations such as conflict detection and resolution in Free Flight [23]. However, only a few have addressed security vulnerabilities in surveillance applications of airborne ad hoc networks [50], [51].

Even with the use of digital signatures, the ATC information assets can be unintentionally corrupted or attacked due to inherent vulnerabilities that are presented next.

B. Addressing Vulnerabilities of ATC

1) Providing Accuracy Information in Signatures: While the accuracy of ADS-B can be significantly higher than radar, making safety-critical ATC operations rely on a position that is computed onboard and communicated over A2A/A2I poses a vulnerability. For example, an inaccurate position that is beyond the expected error margins can disrupt conflict detection and resolution algorithms which compute local safe separation between airplanes [23].

The position, velocity and other spatial data in the beacons is derived from multiple onboard sources, e.g., positioning, altitude and heading systems. The overall accuracy of this data is dependent on the correctness and robustness of these sources as well as security of the data transfer over in-aircraft network. Therefore, as noted in [48], the signed ATC asset must also include the accuracy of the spatial information in order to establish error margins.

2) Enabling Position Verification: A malicious adversary can however attempt to spoof aircraft positions, i.e., make false position claims, to the ground controllers and airplanes. For example, by using a compromised general aviation aircraft equipped with ADS-B or Universal Access Transceiver or by using unattended ground ADS-B equipment [50], [51].

Initial defense mechanisms have been proposed to verify position information received in A2I-Out applications. In [50], a solution approach is proposed that combines two multilaterations at the ground controller, one from use of Time of Arrival of the aircraft beacons and another from that enabled by ADS-B. This solution however, requires at least 4 ground controllers to verify the 3-D position by multilateration. Therefore, it has limited applicability to Free Flight in remote areas where coverage is not as dense. Another solution applicable to the terminal area is the use of secondary surveillance radar for verifying position information received from airplanes [51]. In [51], an approach for position verification of airplanes in Free Flight is proposed. This makes use of ADS-B enabled multilateration in combination with Kalman filter estimation of the flight trajectory based on the bearing information of the source making the position claim. However, the approach needs an additional dedicated omni-directional antenna onboard, to obtain the heading information.

On the other hand, solutions for verification of position information received in A2I/A2A-In applications do not currently exist. The problem is made challenging due to the difficulty of using time of arrival based multilateration in a mobile aircraft, as well as potential for spoofing on the A2I link from ground controller [50]. Most safety threatening situations, such as mid-air collisions, can be potentially mitigated by relying on onboard Traffic Collision and Alerting System transceiver that can interrogate transceivers of neighboring airplanes [48]. However, we note that, as seen in Section VI-C.2, spoofing can be used to delay communications over multi-hop routes in the airborne ad hoc network, which in turn reduces information reachability and its safety benefits [24]. Therefore, the design of position verification mechanisms for A2I/A2A-In applications is pivotal. A potential solution is to build on the approach in [51], and ensure that more information apart from only heading, e.g., range and intended destination, of the claimer is available to the verifier.

C. A Major Challenge in ATC

Even with the increase of automation, the human-in-the-loop will continue to play an important role in controlling the commercial airplane in the AIADS. However, for airplane safety, apart from securing information assets, it is also pivotal to properly present delivered information to the pilot who is an overloaded user. With the enormous amount of information available from the A2I-Out and A2I/A2A-In applications, a major challenge lies in the design of a suitable interface that can provide a coherent and correct presentation to the flight and ground crew controlling the airplane [49].

VIII. Challenges in E-enabled Airplane Security

We present some major challenges in onboard and ground systems due to AIADS constraints in Section III-C.

A. Enabling the Use of Digital Signatures

Digital signatures require a Public Key Infrastructure (PKI), a mechanism that manages identities with associated cryptographic keys and digital certificates [18]. However, the use of a PKI raises issues with the interoperability between multiple CAs and the standardization of certificate policy for aviation to enable global seamless air travel, such as establishment of a "bridge of trust" between unique trusted third parties and development of a policy for various use-cases encountered by the e-enabled airplane [11]. Moreover, as seen later in Section VIII-E, PKI can limit the assurance level of the AIADS.

Further, over the aircraft lifetime, increase in cryptanalytic capabilities of the adversary can also increase the potential

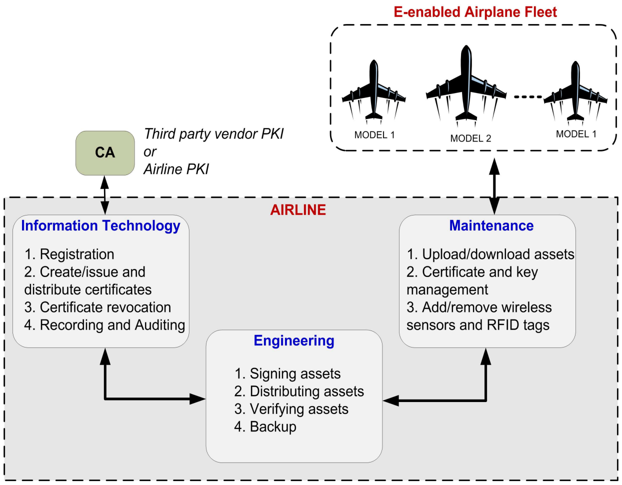

Fig. 6. Illustration of a possible integration of some operational tasks associated with the e-enabled airplane to the existing typical infrastructure and organizational structure of airlines.

for compromise of the signing. Hence to accordingly elongate lifetime of AIADS asset signatures, mechanisms such as periodic key refresh, longer keys or provably secure/forward secure signature algorithms must be considered.

B. Enabling Global Onboard Verification of Signatures

At each traversed airport, the e-enabled airplane may not have guaranteed network access. In the presence of network connectivity, the airplane communicates with multiple off-board systems. Each access point can be shared by multiple airlines at that airport. Additionally, the airplane will receive software from multiple suppliers of the onboard equipment. With the use of digital signatures, this multi-domain problem reduces to ensuring onboard validation of certificates received with the asset for verifying asset signature, even in the absence of networks. Potential solution approaches include the use of a PKI or pre-loaded certificates on the airplane [18]. However, this problem is further complicated in the ATC context, due to the large number of airplanes that can be encountered by each aircraft, as well as the real-time constraints of the control network for verification of the received assets. Further, the scalability of solutions to enable secure verification of received ATC assets at ground controllers can be an issue.

C. Impact of Key and Certificate Management on Airlines

The introduction of certificates and keys in onboard storage clearly affects the e-enabled airplane operator guidance and levies new requirements on airlines, including the need for a PKI [18]. Consequently, airlines may need guidance to cover emerging needs of the e-enabled airplane, such as for distribution and update of certificates and keys.

Fig. 6 illustrates a potential allocation of anticipated operational requirements imposed on the airlines by the e-enabled airplane [18]. To minimize overhead, these requirements are integrated into a typical infrastructure and processes at many airlines. Based on the approach taken by the airlines to handle certificates, there can be an ad hoc solution, i.e., use of preloaded certificates that do not employ a trust chain, or a structured solution, i.e., use of a PKI. Accordingly, the airline CA issuing the trusted certificates, may be an offline third party vendor from which certificates are purchased or an online entity that is external or internal to the airlines.

The distribution of keys and trusted certificates to airplanes can be challenging. This distribution must be protected either by a secure online or out-of-band mechanism. A potential solution approach is to enable onboard generation of the airplane private key and to ensure authentic distribution of the corresponding certificate request to the CA of the airlines, or authentic distribution of the airplane self-signed certificate to all off-board components which require it for verification of assets. Similarly, integrity and authenticity of trusted certificates must be protected during distribution to onboard storage.

The security of the AIADS depends on the integrity and authenticity of trusted certificates and the confidentiality of private keys. However, an airplane may interface with multiple networks and the embedded systems storing airplane keys and certificates may be replaced as needed over the airplane life cycle. These constraints require careful consideration to protect the airplanes private key. Further, compromise of a ground system or an airplane's private key requires that that entity's certificates are revoked to prevent misuse of signatures in the AIADS. Consequently, the e-enabled airplane must be able to validate certificate status periodically or on demand.

D. Impact of Security on Safety

Although existing literature such as [52], [53], [54] argue for commonality among the safety and security disciplines, it remains an open problem as to how the two fields can be integrated. While indeed security affects safety, it is not clear how to express the relevant security considerations and accommodate security risks and mitigations in a safety analysis. Security threats are not bounded and their impact can change over time, making traditional quantitative, probabilistic safety analysis inapplicable for security evaluation [20]. The formulation of guidelines for assessing safety-critical systems along with their security needs would hence require approaches that can integrate the typically discrete methods of security analysis into the quantitative, probabilistic methods [10].

E. High Assurance for AIADS Applications

For airplane safety, the threat level to AIADS assets is that of international terrorists, i.e., sophisticated adversary with moderate resources who is willing to take significant risk [33]. Failure from corrupted safety-critical assets, e.g., loadable software assigned Level A of [13], can be catastrophic. Therefore, according to [33], the integrity and authenticity of safety-critical assets should be guaranteed by the AIADS at an evaluation assurance level of 6 [33]. However, realizing this assurance level can be challenging since evaluation of commercially available PKI is currently limited to the level 4. Further, level 6 requires consideration for the use of formal methods to model and verify systems supporting the EDS.

Airlines business threat level, however, is that of organized crime, hackers, and international corporations, i.e., sophisticated adversary with moderate resources who is willing to take little risk [33]. Hence, the evaluation assurance level 4 is enough to evade business concerns in the AIADS [33].

An assurance level of 6 incurs a significant evaluation effort for systems handling safety-critical assets, including at the airlines. Therefore, an architecture-based solution is needed to reduce costs and time for evaluation of airline systems. As suggested in [10], a potential solution is a two-level approach where the AIADS mechanisms for the most critical security requirements, i.e., integrity, authenticity and authorization for asset corruption threat in Table II, reach an evaluation assurance level of 6, while the remaining components are kept at level 4. This approach enables the design of an architecture that can isolate mechanisms requiring high-evaluation, reducing the evaluation effort at the airlines.

F. Securing Wireless Networked Control of Airplane

A future extension of a wireless-enabled AHM can be in the real-time networked control of the e-enabled airplane [46]. Wireless sensors and actuators can be used as field devices for non-safety-critical controls. The field devices can be integrated with other onboard AHM components in Fig. 4 to form a distributed control system that enables localized computations and actuation (e.g., local temperature control). The system includes a data network, i.e., interconnected wireless sensors, tags and readers, as well as the control network.

Although both data and control networks are subject to the same threats, the impact of these threats on the control network is more critical. For example, by incurring delays or jamming packets in the control network, the adversary can create instabilities and unwanted responses in the control system [46], [47], directly affecting airplane operation. However, most of the current approaches analyzing the stability of networked control systems consider delays [46] and packet losses [47] arising from queuing and congestion in the network. They do not consider the presence of a malicious adversary that is disrupting the control network communications to cause system instabilities. For example, in [46], a dynamic network resource scheduling algorithm for time-critical information sources in a control system is proposed, but the modeled delay is only due to the scheduling and not malicious disruptions. In order to protect communications and prevent unauthorized access to the wireless control network, a promising approach is in multi-layer security, including at physical layer.

IX. Conclusions

The e-enabled airplane with its A2I and A2A applications is envisioned to revolutionize commercial aviation by facilitating rapid advances in next-generation air transportation systems. However, the use of wireless and off-the-shelf technologies introduce vulnerabilities that mandate careful security considerations due to the potential airplane safety and airline business concerns. Further, the resulting security needs and mechanisms must be integrated into the well-defined processes related to airplane operation, control and maintenance.

Previous works have focused on securing the distribution of airplane information assets over the in-aircraft network. However, new threats to the integrity of these assets emerge from A2I and A2A applications including EDS, AHM and ATC. In this paper, we presented a framework to evaluate the security of these applications. We summarized a security evaluation methodology to integrate EDS for supporting current and future commercial airplanes. We also considered emerging threats from potential use of wireless sensors and RFID tags for AHM as well as for wireless networked control of airplane. Furthermore, we reviewed the security challenges with air traffic surveillance applications based on A2A/A2I data links such as 1090 MHz ADS-B, solutions to which can enormously benefit future ad hoc networking of airplanes.

Finally, we consider this paper to be a precursor to a cyber-physical system view of aviation information systems [55].

Acknowledgments

The authors would like to thank Richard V. Robinson, Mingyan Li, Scott A. Lintelman and Chuck Royalty from The Boeing Company, and David von Oheimb from Siemens Corporation for collaborating on the electronic distribution of loadable software. The work presented in this paper was supported in part by ARO PECASE grant W911NF-05-1-0491, ARO grant W-911NF-07-1-0287 and Boeing grant 207946. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors, and should not be interpreted as the views of the U.S. Army Research Office, or the U.S. Government, or The Boeing Company.

References

[1] International Air Transport Association fact sheet – economic and social benefits of air transport. [Online]. Available: http://www.iata.org/pressroom/facts_figures/fact_sheets/economic_social_benefits.htm

[2] Airports Council International Media Release. [Online]. Available: http://www.airports.org/aci/aci/file/Press%20Releases/2007_PRs/PR_180707_WATR.pdf

[3] Next Generation Air Transportation System. [Online]. Available: www.jpdo.gov/

[4] Advisory Council for Aeronautics Research in Europe. [Online]. Available: www.acare4europe.org/

[5] C. Wargo and C. Dhas, "Security considerations for the e-enabled aircraft," *Proceedings of Aerospace Conference*, 2003.

[6] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2001.

[7] H. Bai, M. Atiquzzaman, and D. Lilja, "Wireless sensor network for aircraft health monitoring," in *Proceedings of Broadband Networks (BROADNET)*, 2004, pp. 748–750.

[8] K. Porad, "Rfid in commercial aviation," *Aircraft technology engineering & maintenance*, vol. 75, pp. 92–99, April/May 2005.

[9] R. Harman, "Wireless solutions for aircraft condition based maintenance systems," *Proceedings of Aerospace Conference*, 2002.

[10] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, J. Busser, and J. Cuellar, "Electronic distribution of airplane software and the impact of information security on airplane safety," in *Proceedings of the International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 2007.

[11] J. Pawlicki, J. Touzeau, and C. Royalty, "Data and communication security standards in practice," in *http://www.ataebiz.org/forum/2006_presentations/StandardsInPractice_All.pdf*, 2006.

[12] Radio Technical Commission for Aeronautics Special Committee 203, Unmanned Aircraft Systems, RTCA Paper No. 006-06/PMC-438, December 16, 2005.

[13] RTCA, Software Considerations in Airborne Systems and Equipment Certification (RTCA/DO-178B), 1992.

[14] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing Model 787-8 airplane; systems and data networks securityisolation or protection from unauthorized passenger domain systems access, [docket no. NM364 special conditions no. 250701SC], Federal Register, vol. 72, no. 71, April 13, 2007. [Online]. Available: http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf

[15] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing Model 787-8 airplane; systems and data networks securityprotection of airplane systems and data networks from unauthorized external access, [docket no. NM365 special conditions no. 250702SC], Federal Register, vol. 72, no. 72, April 16, 2007. [Online]. Available: http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf

[16] FAA policy for passive-only RFID devices. [Online]. Available: http://rgl.faa.gov/Regulatory_and_Guidance_Library/ rgPolicy.nsf/0/495367dd1bd773e18625715400718e2e!OpenDocument

[17] R. Robinson, K. Sampigethaya, M. Li, S. Lintelman, R. Poovendran, and D. von Oheimb, "Challenges for it infrastructure supporting secure network-enabled commercial airplane operations," in *Proceedings of AIAA Infotech@Aerospace Conference*, 2007.

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

[19] Aeronautical Radio Inc. (ARINC), Electronic Distribution of Software (ARINC 666), 2006.

[20] G. Bird, M. Christensen, D. Lutz, and P. Scandura, "Use of integrated vehicle health management in the field of commercial aviation," in *Proceedings of NASA ISHEM Forum*, 2005.

[21] K. Sampigethaya, M. Li, R. Poovendran, R. Robinsin, L. Bushnell, and S. Lintelman, "Secure wireless collection and distribution of commercial airplane health data," in *Proceedings of Digital Avionics Systems Conference (DASC)*, 2007.

[22] R. Domingo, "Health monitoring and management systems (HMMS)," in *US/Europe International Aviation Safety Conference*, 2006.

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

[24] M. Cheng and Y. Zhao, "Connectivity of ad hoc networks for advanced air traffic management," *Journal of Aerospace Computing, Information, and Communication*, vol. 1, no. 5, pp. 225–238, 2004.

[25] J. Burbank, R. Nichols, S. Munjal, R. Pattay, and W. Kasch, "Advanced communications networking concepts for the national airspace system," *Aerospace, 2005 IEEE Conference*, pp. 1–19, 2005.

[26] RTCA Special Committee 186 (SC-186) ADS-B support. [Online]. Available: http://adsb.tc.faa.gov/ADS-B.htm

[27] N. Thanthry and R. Pendse, "Aviation data networks: security issues and network architecture," *Security Technology, 2004. 38th Annual 2004 International Carnahan Conference on*, pp. 77–81, 2004.

[28] M. Olive, R. Oishi, and S. Arentz, "Commercial Aircraft Information Security – An Overview of ARINC Report 811," *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA*, pp. 1–12, 2006.

[29] C. Royalty, "Computing security policies and objectives for an airborne information network," in *Aircraft Data Network 664 Working Group*, 2002.

[30] RTCA SC 203, Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDs) on Aircraft (RTCA/DO-294B), December 2007.

[31] SAE, Passive RFID Tags Intended for Aircraft Use (SAE AS5678), December 2006.

[32] RTCA SC 186, Minimum Aviation System Performance Standards (MASPS) for ADS-B, Revision A (DO-242A), June 2002.

[33] Information Assurance Technical Framework, Release 3.1. US National Security Agency. [Online]. Available: http://www.iatf.net/framework_docs/version-3_1/

[34] Common Criteria. [Online]. Available: http://www.commoncriteriaportal.org

[35] J. Ou and H. Li, "Wireless sensor information fusion for structural health monitoring," *Proceedings of SPIE*, vol. 5099, pp. 356–362, 2003.

[36] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[37] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 41–47.

[38] P. Tague and R. Poovendran, "A canonical seed assignment model for key predistribution in wireless sensor networks," *Communications of the ACM*, vol. 3, no. 4, October 2007.

[39] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27–59, 2007.

[40] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 1307–1315, 2007.

[41] L. Lazos and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 1, no. 1, pp. 73–100, 2005.

[42] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," *Proceedings of the 2003 ACM workshop on Wireless security*, pp. 1–10, 2003.

[43] L. Lazos, R. Poovendran, and S. Čapkun, "ROPE: robust position estimation in wireless sensor networks," in *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, 2005, p. 43.

[44] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Security in Pervasive Computing*, pp. 201–212, 2003.

[45] L. Lazos and R. Poovendran, "Power proximity based key management for secure multicast in ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 127–148, 2007.

[46] G. Walsh, H. Ye, L. Bushnell, C. Technol, and C. Oakland, "Stability analysis of networked control systems," *Control Systems Technology, IEEE Transactions on*, vol. 10, no. 3, pp. 438–446, 2002.

[47] B. Azimi-Sadjadi, "Stability of networked control systems in the presence of packet losses," *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, vol. 1, 2003.

[48] E. Lester and J. Hansman, "Benefits and incentives for ADS-B equipage in the national airspace system," *MIT ICAT Report, ICAT-2007-2*, 2007.

[49] D. W. Nelms, "Airframer advances surveillance techniques," *Avionics Magazine*, October 1, 2007.

[50] M. Sharples, H. Hutchinson, K. Carpenter, and D. Bowen, "Integrity and security of ADS-B," in *SurTech*, 2004.

[51] J. Krozel and I. Andrisani, "Independent ADS-B Verification and Validation," *AIAA 5 th Aviation, Technology, Integration, and Operations Conference(ATIO)*, pp. 1–11, 2005.

[52] S. Brostoff and M. Sasse, "Safe and sound: a safety-critical approach to security," in *Proceedings of the ACM workshop on New Security Paradigms*, 2001, pp. 41–50.

[53] A. Pfitzmann, "Why safety and security should and will merge, Invited talk," in *Proceedings of the International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 2004.

[54] V. Stavridou and B. Dutertre, "From security to safety and back," in *Proceedings of the Conference on Computer Security, Dependability and Assurance*, 1998, pp. 182–195.

[55] S. Lintelman, K. Sampigethaya, M. Li, R. Poovendran, and R. Robinson, "High Assurance Aerospace CPS and Implications for Automotive Industry," *Proceedings of the National Workshop on High Confidence Automotive Cyber-Physical Systems (CPS)*, April 2008.

Appendix

TABLE IV

Common Abbreviations in this Paper

A2A	Aircraft-to-Aircraft Communication
A2I	Aircraft-to-Infrastructure Communication
ADS-B	Automated Dependent Surveillance Broadcast
AHM	Aircraft Health Management
ATC	Air Traffic Control
CA	Certificate Authority
CC	Common Criteria
EDS	Electronic Distribution of Loadable Software
FAA	Federal Aviation Administration
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
WSN	Wireless Sensor Network