A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance [*]

Krishna Sampigethaya

Boeing Research & Technology, Bellevue, WA, 98008, USA

Radha Poovendran

Network Security Lab (NSL), EE Dept., University of Washington, Seattle, WA, 98195, USA

Linda Bushnell

Networked Control Systems Lab, EE Dept., University of Washington, Seattle, WA, 98195, USA

Current air traffic management systems suffer from poor radar coverage and a highly centralized architecture which can under heavy traffic loads overwhelm Air Traffic Control (ATC) centers. Such limitations can lead to inefficient use of the available airspace capacity and insecure scenarios such as low-visibility landings. Future air transportation systems with e-enabled aircraft and networked technologies, such as Automated Dependent Surveillance Broadcast (ADS-B), are cyber-physical systems that promise to help reduce traffic congestion and ATC inefficiencies by enabling exchange of precise surveillance data in shared airspace. This paper focuses on cyber security concerns with highly accurate surveillance of aircraft navigating in a future shared space. A framework is proposed to protect traffic data for both ground and airborne surveillance of aircraft. The framework identifies major threats and vulnerabilities from cyber exploits, specifies security requirements and mitigation solutions. Major security challenges anticipated in supporting networked infrastructure are given along with some open problems.

I. Introduction

Skies have become more crowded in the last decade. Current air traffic management infrastructures are however close to their life's end, with system software, hardware, architectures and network links not possessing the growth capacity to meet demands of future aviation. The next-generation air transportation systems, such as NextGen in the USA[1] and SESAR in Europe,[2] will employ technologies and processes for enhancing airspace capacity and aircraft operation. In these future systems, the e-enabled aircraft is envisioned to play a key role with its advanced sensing, computing and communications features.[3]

The e-enabled aircraft will use the Asynchronous Dependent Surveillance Broadcast (ADS-B), based on the Global Positioning System (GPS) and digital links ranging up to 100 miles, to automate and decentralize Air Traffic Control (ATC) tasks. Each aircraft periodically broadcast a beacon as frequent as once or twice every second.[5,30] The beacon contains an identifier and the current state of the aircraft, i.e., position, altitude, intent, velocity, time and other information. These beacons can be utilized at the ground controllers and navigating aircraft for highly accurate *ground and airborne surveillance*, respectively. Ground controllers can also send traffic information to aircraft even in remote mountainous and oceanic regions. The overall gain in situational awareness can help to optimize air travel time and costs. En-route aircraft can engage in Free Flight, i.e., self-optimize by choosing its route, altitude, or velocity,[21] traffic flows at a congested terminal area can be optimized, and ground delays at the gates, taxiways and runways can be reduced;[29] see Fig. 1.

[*] 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 Boeing Company.

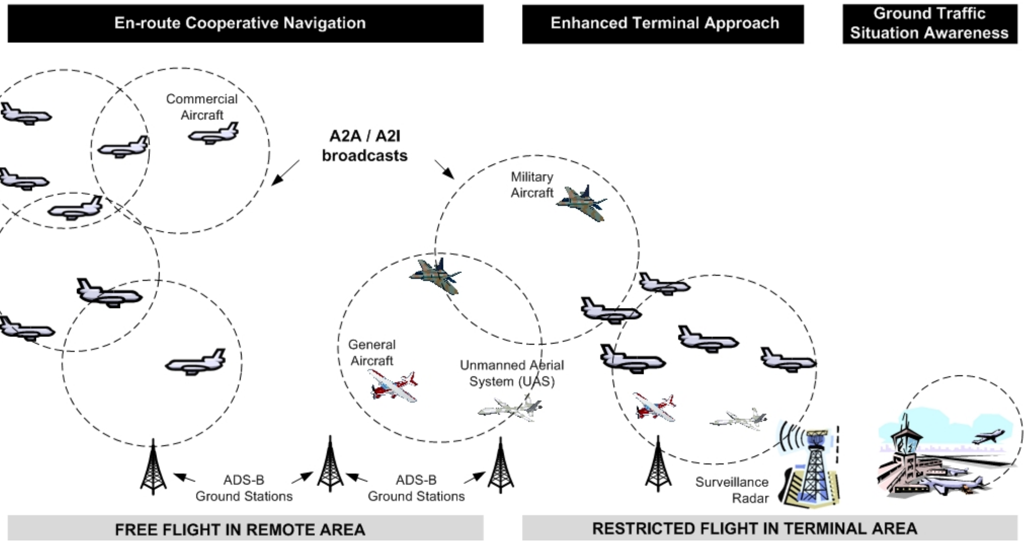
En-route Cooperative Navigation
Enhanced Terminal Approach
Ground Traffic Situation Awareness
Commercial Aircraft
A2A / A2I broadcasts
Military Aircraft
General Aircraft
Unmanned Aerial System (UAS)
ADS-B Ground Stations
ADS-B Ground Stations
Surveillance Radar
FREE FLIGHT IN REMOTE AREA
RESTRICTED FLIGHT IN TERMINAL AREA

Figure 1. Illustration of a future air transportation system with e-enabled aircraft, aircraft-to-infrastructure & aircraft-to-aircraft communications and applications.

Before their wide-scale deployment, any airborne or ground-based technology must be ensured to have no impact on safe and expected operation of the system. Today however there is lack of a clear understanding of how emerging cyber-world technologies, such as ADS-B and radio frequency identification (RFID), with their vulnerabilities can impact airworthiness and aircraft operator business,[8,9,11] impeding their beneficial application. As a recent example, the FAA regulated only the use of passive RFID tags for aircraft-on-the-ground scenarios, until the impact of active tags on other onboard systems is clearly determined.[10] Similarly the beneficial use of ADS-B is currently limited to some ground surveillance tasks. ADS-B will openly broadcast identifiable aircraft positions as well as utilize aircraft positions received over a shared link, hence requiring a full assessment of threats from unauthorized access and unanticipated disruptions before it can potentially inform more critical navigation tasks such as in airborne surveillance.[11]

This paper proposes a framework for streamlining threat assessment for ADS-B and other future surveillance broadcast technologies. The remainder of this paper is organized as follows. Section II overviews the major research and development efforts as well as ongoing standards for securing networks and operations for the e-enabled aircraft. Section III describes the future ATC system model considered. Section IV presents the proposed framework for security assessment of ground and airborne surveillance of e-enabled aircraft. Section V lists some major challenges, open problems and future research. Section VI concludes the paper.

II. Related Work

A. Ongoing Research for Securing the e-Enabled Aircraft

Several research efforts aim to develop an understanding of the security needs of networked systems and applications of the e-enabled aircraft. A framework based on the Common Criteria standard methodology has been establish to specify requirements for protecting the distribution of loadable software and data between aircraft and airline ground systems as well as end-to-end distribution between aircraft and software suppliers against threats to airworthiness and airline business.[4] Secure integration of emerging wireless technologies with the e-enabled aircraft are also being considered, such as use of onboard wireless sensor networks and RFID tags for aircraft health management.[7,14,15] Further, the anticipated impact of the use of security solutions on the commercial aviation information systems and processes are being identified.[19] An abundance of literature also addresses the airborne point-to-point networking issues, such as transmission protocol design and the impact of air traffic density on the network topology,[22,23] as well as the design of safety-critical ATC operations such as conflict detection and resolution in Free Flight.[21] However, only a few have just begun to address security and reliability of future ATC based on broadcast data links, for mitigating threats to data integrity and authenticity in ADS-B based navigation and surveillance.[16,31]

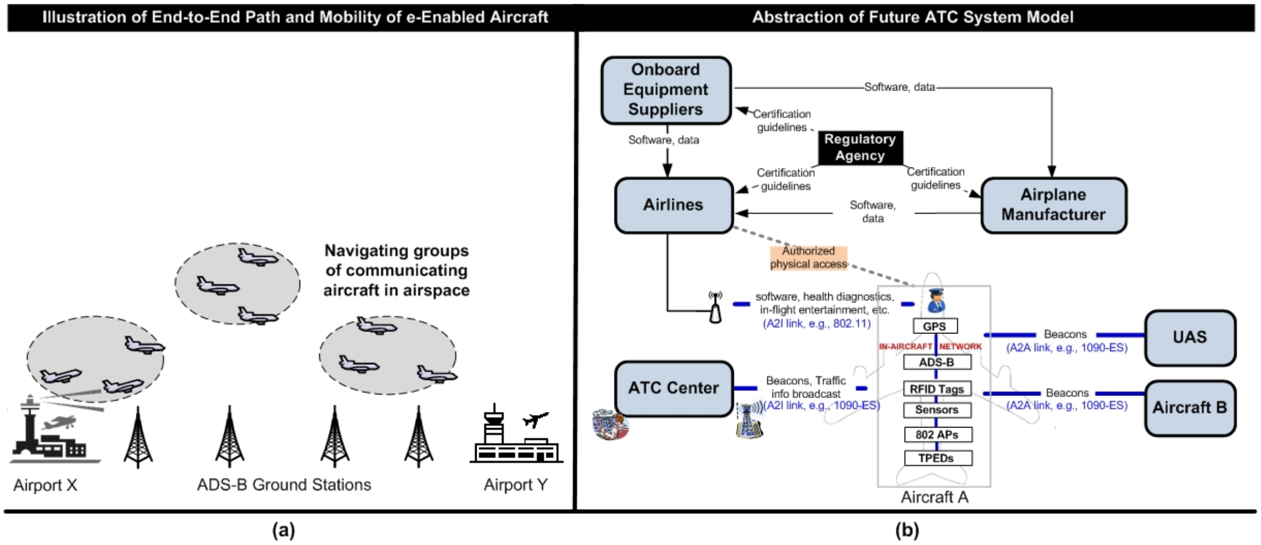
Illustration of End-to-End Path and Mobility of e-Enabled Aircraft
Navigating groups of communicating aircraft in airspace
Airport X
ADS-B Ground Stations
Airport Y
(a)
Abstraction of Future ATC System Model
Onboard Equipment Suppliers
Software, data
Certification guidelines
Regulatory Agency
Software, data
Certification guidelines
Certification guidelines
Airlines
Software, data
Airplane Manufacturer
Authorized physical access
software, health diagnostics, in-flight entertainment, etc.
(A2I link, e.g., 802.11)
GPS
IN-AIRCRAFT NETWORK
ADS-B
RFID Tags
Sensors
802 APs
TPEDs
Aircraft A
Beacons
(A2A link, e.g., 1090-ES)
UAS
ATC Center
Beacons, Traffic info broadcast
(A2I link, e.g., 1090-ES)
Beacons
(A2A link, e.g., 1090-ES)
Aircraft B
(b)

Figure 2. (a) Illustration of group navigation behavior of aircraft traversing the shared airspace. (b) A high-level abstraction of a future air traffic control system model with the e-enabled aircraft which can exchange onboard equipment software updates and data with entities outside air traffic management.

B. Emerging Security Standards for the e-Enabled Aircraft

Major security standards are being developed for the e-enabled aircraft and its networked systems. ARINC 811 recommends an aircraft network architecture that securely separates the flight critical systems from others and also presents a framework to identify protection mechanisms for in-aircraft network that can account airline needs and constraints.[25] RTCA Special Committee SC-202 is now considering the interference from onboard transmitting personal electronic devices (e.g., cellular devices, active RFID tags, embedded medical sensors) on the aircraft, and making recommendations for their use in RTCA DO-294B. Further, SAE AS5678 is a developing standard which identifies requirements for the use of passive RFID tags onboard and currently recommends use of password based mechanisms for RFID tag security. For exchanges between aircraft and ground systems, ARINC 827 is currently defining the data format for electronic delivery of signed loadable software and other related information. ARINC 623 specifies the format for air traffic messages that are sent on point-to-point ACARS data link, and ARINC 823 provides a framework for securing ACARS messages transmitted between aircraft and ground systems. Recently RTCA SC-186 has taken on the role of standardizing ADS-B and its commercial aviation implementations based on 1090-ES broadcast data link, while a variety of ADS-B applications are in RTCA DO-242A.

III. System Model

Fig. 2 illustrates a high-level abstraction of a future ATC system considered in this paper. We assume the e-enabled aircraft has onboard systems to compute and update highly accurate actual position information for navigation and surveillance. ADS-B provides a broadcast data link between aircraft and ATC centers (aircraft-to-infrastructure communications or A2I) as well as between aircraft (aircraft-to-aircraft communications or A2A) for surveillance, with a one-hop communication range of 40 to 90 nautical miles, e.g., 1090 MHz Extended Squitter datalink.[22] Apart from aircraft periodic beacons, the ADS-B links are used to communicate traffic information broadcasts from ground controllers such as real-time weather and locations of aircraft with no ADS-B units.[29] The reachability of this traffic information can be extended via multi-hop communications between aircraft.[22]

The enabled applications in this ATC system model can be generally classified to be A2I-Out if aircraft is only broadcasting data, or A2A/A2I-In if aircraft is broadcasting data as well as utilizing/forwarding data in received broadcasts. Ground surveillance using ADS-B is an A2I-Out application. Whereas, airborne surveillance and traffic information service using ADS-B are A2A/A2I-In applications.

A. System Assumptions

Access to the air traffic management system is assumed to be controlled properly. It is also assumed that cryptographic and security quantities are properly maintained and protected. Sufficient protection is provided for robustness against well known denial of service attacks. In case of ADS-B failures, secondary or primary surveillance radar coverage is assumed to be available and adequate to meet minimum operating requirements for ATC. Further, airlines are assumed capable of managing onboard network and security configurations in a reliable and correct manner. Sufficient checks are in place to prevent unauthorized physical access to onboard systems. Additionally, the ground controllers are assumed to properly conduct the traffic management tasks.

B. System Constraints Considered

Any solution approach for securing aircraft surveillance must account for the following major constraints of the e-enabled aircraft.

Regulatory Constraints. Aviation is subject to a well-established stringent regulatory environment to assure that aircraft safety and public well being are protected. Regulatory agencies, such as the FAA, set mandatory guidelines that must be met for the aircraft to be considered airworthy and flight-ready. Any new cyber technology for aircraft must be shown to have no impact on safe operation of the aircraft. As a result, proposed solutions and requirements must be integrable with current well-defined regulations and capable of meeting minimum operating standards for ATC.

Path Constraints. The end-to-end flight path of an aircraft can be separated into different traffic management operational phases such as terminal departure, en-route, terminal approach, terminal arrival, etc. The time period of each phase is usually pre-determined but can vary due to ATC negotiations and other external uncertainties. Further, the time criticality of communications is different for each operational phase. For instance, the ADS-B broadcasts can be less frequent when aircraft is in en-route phase (e.g., a beacon per second) rather than terminal approach phase (e.g., two beacons per second). Nevertheless, proposed solutions are expected to perform within these path constraints. Furthermore, the traversed airspace varies in aircraft density, for instance terminal areas exhibit higher densities compared to en-route regions, which means that flexibility of flight paths can vary based on the current occupied airspace.

Mobility Constraints. Airplanes mostly follow predictable routes, except possibly during Free Flight, and travel in an pre-flight established trip time. Therefore, aircraft traversing in a similar direction and within one-hop communication range can be expected to be an ad hoc navigating group of nodes forming a fully connected network graph within the group for relatively long time periods.

Message Size Constraints Based on the current standards for ADS-B links, a broadcast surveillance message size can vary in order of only a few tens to several hundreds of bytes, e.g., for ADS-B UAT link maximum size for aircraft traffic beacons is 34 bytes and for traffic information broadcasts from ground is 554 bytes.[16]

Cost Constraints. System operation and maintenance costs must be reduced at the different stakeholders. Therefore, any proposed solution must minimize overhead. Further, to obtain a return-of-investment on existing ATC systems and processes, any new technology and solution must be compatible with them.[20]

Table 1 summarizes some of the major implications of these constraints for future surveillance technologies such as ADS-B.

C. Adversary Model Considered

The overall objective of the adversary is to degrade performance and accuracy of the ATC system by attacking its traffic information assets, e.g., motivation of hackers or criminal organizations. The use of a wireless broadcast datalink in the ATC system provides easy open access to traffic communications, allowing attacks to create unexpected behaviors in and loss of highly accurate surveillance. For simplified analysis, we consider attacks to be only over the wireless links in the system. The adversary can be external to the ATC

Table 1. ATC system constraints and implications for future broadcast surveillance technologies.

Constraint	**Implications for Future Broadcast Surveillance**
Regulatory constraints	Guidelines for security management
Path constraints	Multilateration availability and accuracy vary during flight Traceability of periodic beacons Computational and communication constraints
Mobility constraints	Group navigation of aircraft
Message size constraints	Maximum size for security parameters
Cost constraints	Processes for security management Lower usage of expensive radars is desired

system, capable of passive eavesdropping of traffic data as well as active attacks such as data corruption, spoofing, and wireless channel jamming, or can be an insider controlling some unattended ADS-B ground stations or a general aviation aircraft equipped with a Universal Access Transceiver for the same attacks.

We note that insider attacks based can be deterred by enforcing legal regulations and sufficiently safeguarded against with specific physical, logical and organizational inhibitors. However, in this paper, we consider threats from external attackers as well as insiders for rigor and completeness of our security analysis. We expect that such an approach can enhance the level of protection to future ATC systems.

IV. Proposed Security Framework

A. Security Threats

(T1) Manipulation of Positioning Systems Readings. The position, velocity and other spatial data in the beacons is derived from multiple onboard sources, e.g., positioning, altitude and heading systems. Attackers may attempt to disrupt and prevent onboard readings, for instance that of the GPS unit, and impact the accuracy or availability of position data in the traffic beacons.

(T2) Manipulation of Traffic Data. Vulnerabilities in ground and airborne surveillance emerge from the dependency of ATC tasks on the integrity of traffic beacons and traffic information broadcasts. In order to incur unwarranted flight delays, unnecessary safety concerns and operational costs in the ATC system, attackers may attempt to intentionally engineer errors in surveillance by corrupting traffic data or spoofing positions. For instance, creating false conflicts by broadcasting bogus aircraft positions using virtual transmitters.

(T3) Exploitation of Traffic Data. The broadcast nature of the periodic traffic beacons can present vulnerabilities exploitable for privacy attacks in some scenarios. For example, using the identifiers in observed traffic beacons in terminal areas an eavesdropper may attempt to generate location profiles and derive other potentially sensitive information of privately operated aircraft owners for personal gains. On the other hand, the eavesdropper may passively use the traffic information broadcasts from ground controllers for further attacks.

(T4) Liability. An entity in the ATC system could deny having broadcast any false traffic data after detection of the manipulation.

(T5) Delay of Multi-hop Traffic Information. If multi-hop routes are employed to extend information reachability of information broadcasts from ground controllers, then attackers may attempt to make this information inaccessible to remote aircraft by creating inefficient routes via either channel jamming or introducing misleading routing messages. For example, if geographic routing is used then by spoofing position information (e.g., the wormhole attack[26]) a compromised node can modify routes as desired by it.

B. Security Requirements

Most safety threatening situations, such as mid-air collisions, can be mitigated in future surveillance by relying on the onboard Traffic Collision and Alerting System (TCAS) transceiver which interrogates corresponding transceivers of neighboring aircraft.[29] In fact, the integration of TCAS and ADS-B is ongoing.[17] Furthermore, the threat from disruption of onboard positioning systems described above can be mitigated by including spatial accuracy parameters in the beacons to establish error margins for computations.[29] However, the following security properties are needed to address the remaining threats.

Integrity and Authenticity. For preventing adversarial manipulation of traffic data, the contents of the broadcast must be verifiable to be the same as at the source. Further, the source identity must also be verified.

Confidentiality. Unauthorized access to traffic information broadcasts from ground controllers whose contents may provide leverage for adversary's personal gain must be prevented.

Early and Correct Detection Any manipulation of traffic data must be detected as soon as possible so as to not disrupt the pre-established time for flight, while also eliminating or reducing false alarms in the detection of manipulation.

Non-repudiation. For establishing liability in the ATC system, each traffic broadcast must be undeniably associated with at least one authentic entity in the system.

Anonymity. Unauthorized tracking of an identifiable aircraft's positions from its traffic beacons must be mitigated when desired.

Availability. Traffic data must be available in time to enable highly accurate and dependable surveillance. A backup mechanism, such as secondary surveillance radar, must be available along with related processes to ensure no complete loss of minimum operating conditions for the ATC system.

We now present potential defense mechanisms that can meet the security requirements and constraints of ATC system.

C. Use of Multilateration Solutions

Multilateration based mechanisms have been proposed to verify position information in A2I-Out traffic beacons received at the ground. A solution approach is to combine 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.[24] This solution works in well covered regions such as terminal areas, where at least 4 ground controllers are available to verify the 3-D position. Another solution for terminal areas is the use of secondary surveillance radar for verifying position information received from aircraft.[31] For remote regions where aircraft are engaged in Free Flight, a promising approach for position verification of aircraft is to use 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.[31] This approach however assumes the availability of a dedicated omni-directional antenna onboard for the heading information.

A2A/A2I-In applications, however, are currently impeded by the dearth of feasible solutions for verification of positions and integrity protection of traffic information received by aircraft via A2A/A2I-In broadcasts. The problem is challenging because of the difficulty of performing time-of-arrival based multilateration in a mobile aircraft as well as potential for easy spoofing over the A2I link from the ground.[24] A potential solution is to enable aircraft to verify positions by ensuring more information, such as heading, range and intended destination, of the claimer is available to the verifier from additional surveillance data sources such as from one or more honest one-hop neighbors.

Table 2. Mapping of security threats, requirements and mitigation solutions. $\surd$ – satisfied; C – partially satisfied; $\times$ – not satisfied. T1 - Manipulation of Positioning Systems Readings; T2 - Manipulation of Traffic Data; T3 - Exploitation of Traffic Data; T4 - Liability; T5 - Delay of Multi-hop Traffic Information

Requirement/Threat	T1	T2	T3	T4	T5	A2I-Out Solution	A2A/A2I-In Solution
Beacon Accuracy	$\surd$	$\times$	$\times$	$\times$	$\times$	Accuracy parameters	Same
Integrity & Authenticity	$\times$	C	$\times$	$\times$	$\times$	Multilateration	Signatures
Confidentiality	$\times$	$\times$	$\surd$	$\times$	$\times$	Symmetric Encryption	Encryption
Early / Correct Detection	$\times$	C	$\times$	$\times$	$\times$	Multilateration	Signatures
Non-repudiation	$\times$	$\times$	$\times$	$\surd$	$\times$	Signatures	Signatures
Anonymity	$\times$	$\times$	$\surd$	$\times$	$\times$	Pseudonyms Group Navigation	Same Same
Availability	$\times$	$\times$	$\times$	$\times$	$\surd$	Radar	Same

Furthermore, multilateration in some situations may have weaknesses, since it is possible to simulate virtual transmitters at a given position by varying the timing of multiple transmitters or offset the position calculation by disrupting clock synchronization of the ground receivers.[18] In such cases, additional mechanisms for position verification, such as primary surveillance radar, can be used. Another promising solution is to employ cryptographic solutions as described next.

D. Use of Cryptographic Solutions

Symmetric-key based solutions offer an efficient means to protect integrity, authenticity and confidentiality of traffic data. One approach applicable to A2I-Out traffic beacons and A2A-In traffic information broadcasts from ground is to use a keyed hash or Message Authentication Code based on a pre-shared secret between aircraft and ground controllers.[16] The shared secret can be used to also encrypt sensitive messages.

Symmetric cryptography however is not viable for A2A/A2I-In traffic beacons due to the impracticality of pre-sharing a secret between airborne nodes. A potential solution approach is to use digital signatures and public key encryption based on efficient asymmetric cryptography such as Elliptic Curve Cryptography. Apart from integrity, authenticity and confidentiality, verifying a signature as soon as it received can contribute to the *early and correct detection* requirement as well as for ensuring *non-repudiation*. We note that asymmetric cryptography solutions can also well serve to protect traffic information from ground controllers, since allowed message sizes here can be in order of several hundred bytes (e.g., approx. 556 bytes for ADS-B UAT). However, use of signatures can be challenging for ATC. In order to verify signatures, the onboard systems must be able to verify the associated digital certificate validity implying the scalability requirement for identifying the large number of nodes that can be encountered by each navigating aircraft. Further, the scalability of solutions to enable secure verification of received assets at ground controllers can be an issue.

E. Use of Pseudonyms and Group Navigation

For gaining anonymity, a temporary identifier called pseudonym can be assigned to an aircraft such that only authorized entities can link the pseudonym with the aircraft's permanent digital identifier. Further, to remove correlation between two consecutive accurate positions of an aircraft, the aircraft can simply update the pseudonym used in the corresponding traffic beacons. However, despite the pseudonym update the aircraft may be traceable due to the temporal and spatial relations between the new and old locations of the aircraft. A prospective solution is to use a random time period between update of pseudonyms.[32]

In order to achieve a random time period for pseudonym update, one approach is to leverage group navigation feature. As noted in Section B, aircraft in geographical proximity with same average velocity and similar direction can navigate as a fully-connected group over a period of time. Such geographically proximate aircraft can continue to broadcast traffic beacons with pseudonyms, while coordinating to be represented by a common valid group identifier for most purposes as well as establishing secrets on-the-fly for group-based operations. Given that the group identifier is only traceable to a navigating group of aircraft and that the members can self update their pseudonyms while participating in the group, each member can potentially achieve a random time period safely for pseudonym update. The ground controllers can still identify and accurately trace valid nodes in the sky, while unauthorized eavesdroppers can at best attempt to predict trajectories of these airborne nodes.

Table 2 shows which threats can be mitigated using the above solution mechanisms for meeting security requirements.

V. Major Challenges, Open Problems and Future Work

This section discusses some of the major security challenges and problems in future ATC systems.

A. Graceful Degradation of Future Surveillance Systems

The design of the proposed solutions and their related procedures must be such that the performance and accuracy of the ATC system can gracefully degrade with increase in the fraction of compromised nodes. Understanding the impact of cyber exploits on airborne surveillance and how to efficiently respond to these exploits remains a major open problem. For instance, upon detection of an exploit, a safe solution is a well-established combination of technology and processes to increase the radius of the circle of avoidance for aircraft from that of ADS-B to a higher value, e.g., that of secondary surveillance radar. Furthermore, the transition must be ensured to be safe even in the presence of malicious nodes in the system. The use of a pessimistic circle of avoidance radius will however enable an attacker to enlarge the impact of an exploit from a terminal area to an entire ATC center.

B. Addressing the Impact of Cryptographic Solutions

Factors such as global spanning flight paths, lack of guaranteed seamless network connectivity, multiple communicating ground stations and aircraft, and maintenance cost constraints can complicate the design of suitable solutions for managing an aircraft's cryptographic keys as well as shared secrets used for validating or encrypting traffic data. Asymmetric cryptography solutions usually require a Public Key Infrastructure (PKI), i.e., a mechanism for managing identities with associated keys and certificates.[19] However, for a large complex system such as the ATC system, PKI gives rise to challenges such as enabling interoperability between multiple CAs and developing a standard certificate policy for multiple scenarios encountered by the airplane.[6] Moreover, evaluating a complex system such as PKI at an assurance level adequate for the ATC system is a major challenge as well. Furthermore, offline verification mechanisms, such as use of pre-loaded certificates, is needed to compensate for any lack of online connectivity between aircraft and the CA. This alternative is however complicated by the need for scalability.

Furthermore, in order to satisfy demands of regulatory bodies and airlines, proper digital certificate and key management processes must be defined. Regulatory agencies understand that the introduction of certificates, keys and shared secrets in the onboard system storage can affect existing guidance for aircraft. Airlines that currently do not fully support any PKI may need guidelines for updating and distributing keys and certificates in avionics.

C. Leveraging Advances in Vehicular Ad Hoc Networks

Even today technological innovations in automotive industry continue to have a positive impact on the aerospace industry. It can be anticipated that the rapid advances currently witnessed in the networking, security and privacy of the emerging vehicular ad hoc networks (VANETs) can significantly benefit the airborne ad hoc networks.[14, 32] For instance, cooperative navigation and collision avoidance applications in VANET have the same objective as their counterparts in an ATC system. Further, group navigation, discussed in Section II.B, is a common property of both networks.[32] Interesting research may lie in leveraging design of secure solutions being developed in VANET, for mitigating threats to the ATC system.

D. Assessing Impact of Security on Safety

Although existing literature argue for commonality among the safety and security disciplines,[33,34] it remains an open problem as to how the two fields can be combined. While security affects safety, it is not clear how to express the relevant security considerations and how to accommodate security risks and mitigations in the context of 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 together with their security needs would therefore require approaches that can integrate the typically discrete methods of security analysis into the quantitative, probabilistic methods.[4]

E. High Assurance for a Complex System

To enable the beneficial and secure use of a system for distribution of critical assets of aircraft, high confidence in the security properties is needed. However, ATC system related factors such as multiple entities involved and the complex interaction between technology components at an entity, make establishment of a high level of confidence a major challenge to overcome. Formal methods (FM) offers a technique towards providing high assurance for the design and development of the aviation cyber systems. However, the cost-effective and time-efficient use of FM for end-to-end evaluation of large and complex systems is a challenging problem. A potential solution approach is to apply formal methods to only the critical components. This approach has been used to analyze the distribution of loadable software for aircraft. However, this approach must overcome two major problems. One, the maximum assurance level of commercially available PKI is currently limited to medium assurance levels, hence requiring the design and implementation of a PKI at that level.[4] Two, high assurance evaluation requires consideration for the use of complex analytical tools which can be time consuming and expensive, giving rise to challenges from cost constraints.[4]

F. Real-Time Networked Control System Design

Most of the current approaches analyzing the stability of networked control systems consider delays[13] and packet losses[28] arising from queuing and congestion in the network. They do not consider the presence of a malicious adversary that is intentionally disrupting the control network communications to create system instabilities. For example, in,[13] a dynamic network resource scheduling algorithm for time-critical information sources in the control system is proposed, but the modeled delay is only due to the scheduling and not other malicious disruptions. However, with the use of vulnerable wireless technologies, the analysis and solutions for networked control system responsible for real-time operations in the aircraft must take into account the emerging threats.

VI. Conclusions

In this paper, we developed a framework for broadcast data link based navigation and surveillance for future e-enabled aircraft. Our security analysis provided a classification of major threats to use of broadcast medium for transmitting accurate aircraft positions and other traffic information. After specifying security requirements, we presented solution approaches based on multilateration for position verification, cryptography for data integrity, authenticity and confidentiality, and pseudonyms and position tracking mitigation for aircraft operator privacy. Multilateration works well for aircraft surveillance by ground controllers if there is sufficient density of ground stations and/or secondary sources for position verification, however its use for airborne surveillance by aircraft is limited. Cryptographic schemes can offer a means to enable secure airborne surveillance, but the schemes must be efficient. The introduction of cryptographic solutions for e-enabled aircraft further places the overhead of properly managing keys, certificates and secrets. In our future work, we will evaluate the effectiveness of the use of pseudonyms and group navigation for protecting anonymity of e-enabled aircraft, as well as study the impact of air traffic control system's cyber exploits on the physical-world parameters such as flight delays and operational costs.

References

[1] Next Generation Air Transportation System. www.jpdo.gov/

[2] Single European Sky ATM Research in Europe. http://www.eurocontrol.int/sesa

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

[4] 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.

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

[6] 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.

[7] Bai, H., M. Atiquzzaman, D. Lilja, "Wireless sensor network for aircraft health monitoring," *Proceedings of Broadband Networks (BROADNETS)*, 2004.

[8] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing model 7878 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., 2007, http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf

[9] Federal Aviation Administration, 2007, 14 CFR Part 25, Special Conditions: Boeing model 7878 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., 2007, http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf

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

[11] Status of FAAs Efforts To Develop the Next Generation Air Transportation System. [Online]. Available: http://www.oig.dot.gov/item.jsp?id=2352

[12] Radio Technical Commission for Aeronautics (RTCA), Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDs) on Aircraft, RTCA/DO-294B.

[13] Walsh, G., Ye, H., Bushnell, L, Stability analysis of networked control systems, *Proceedings of American Control Conference*, 1999, pp.2876-2880.

[14] Sampigethaya, K., Poovendran, R., Bushnell, L. Secure operation, maintenance and control of future e-enabled airplanes, *Proceedings of the IEEE*, Vol. 96, No. 12, Dec. 2008, pp. 1992-2007.

[15] Li, M., Poovendran, R., Falk, R., Kopf, A., Sampigethaya, K., Robinson, R., and Lintelman, S., Multi-Domain RFID Access Control Using Asymmetric Key Based Tag-Reader Mutual Authentication, *Proceedings of the 26th Congress of the International Council of the Aeronautical Sciences (ICAS)*, September 2008.

[16] Valovage, E., Enhanced ADS-B Research, *IEEE Aerospace and Electronic Systems Magazine*, vol.22, no.5, pp.35-38, May 2007.

[17] RTCA, Special Committee 218 Terms of Reference, Future ADS-B / TCAS Relationships, RTCA Paper No. 095-08/PMC-619, March 13, 2008.

[18] Haley, C.B.; Laney, R.; Moffett, J.D.; Nuseibeh, B., Security Requirements Engineering: A Framework for Representation and Analysis, *IEEE Transactions on Software Engineering*, vol.34, no.1, pp.133-153, Jan.-Feb. 2008.

[19] 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.

[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] 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.

[22] 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.

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

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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

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

[31] 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.

[32] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE Journal on Selected Areas in Communications*, 25:8, p. 1569, 2007.

[33] 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.

[34] 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.