# Security of Future eEnabled Aircraft Ad hoc Networks

Krishna Sampigethaya
*Boeing Phantom Works, Bellevue, WA, 98006, 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* *

**This paper focuses on security concerns with a future ad hoc network of data linked eEnabled airplanes, and proposes a framework to protect communications. The framework identifies emerging threats and vulnerabilities, specifies security requirements and mitigation solutions. Major security challenges anticipated in the ground infrastructure and eEnabled airplanes are presented along with some open problems.**

## I. Introduction

Aviation is today faced with major challenges due to an unprecedented increase in air traffic, such as airspace congestion, fuel costs and environmental pollution. Consequently, several large-scale initiatives have begun to build next-generation air transportation systems that will have improved capacity and capabilities over the next two decades. For example, the collaborative effort called NextGen between the Federal Aviation Administration (FAA) and other federal agencies, industry and academia in the USA,[1] and the Advisory Council for Aeronautics Research in Europe.[2]

In these emerging air transportation systems, the *eEnabled airplane* promises to revolutionize air travel.[3] The eEnabled airplane will possess advanced avionics and cost-effective off-the-shelf wireless solutions for enhancing operation, maintenance and control. For example, the Global Positioning System (GPS) and Automated Dependent Surveillance Broadcast (ADS-B) for air traffic control,[4,6] wireless access points for electronic distribution of software and data,[22] Radio Frequency Identification (RFID) and wireless sensors for health monitoring.[7,9,10] With such unprecedented features, the eEnabled airplane is envisioned to participate as a self-aware node in a Aircraft Ad hoc Network (AANET), ubiquitously communicating with ground infrastructure and other airplanes. The enhancements in information delivery and availability from in-aircraft, aircraft-to-ground and aircraft-to-aircraft communications in the AANET can improve areas such as flight safety, schedule predictability, maintenance and operational efficiencies, passenger amenities.

However, off-the-shelf wireless solutions can open vulnerabilities that give rise to security concerns with the eEnabled airplane. The ease of accessibility to wireless communications allows unauthorized remote access, providing new opportunities for attackers to manipulate data without physically accessing the onboard systems. For example, a malicious attacker may attempt to corrupt airplane data during their distribution in the AANET, such as onboard executable software specified in Radio Technical Commission for Aeronautics (RTCA) DO-178B, to degrade airworthiness and/or impede beneficial operation.

Current well-established regulations and guidelines for continued airworthiness of airplanes do not yet cover emerging vulnerabilities from onboard wireless solutions.[11,12] Safety concerns with these solutions are focused on the impact of radio interference on onboard systems operation, requiring isolation or prevention

*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.

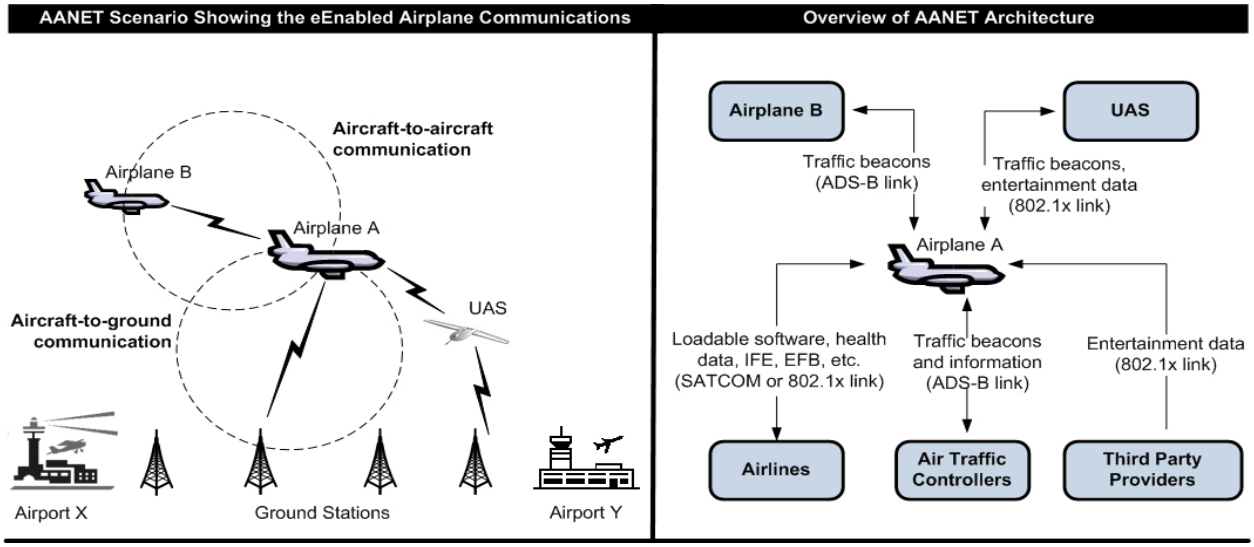


**Figure 1. Illustration of a future air transportation system with eEnabled airplanes, aircraft-to-ground & aircraft-to-aircraft communications, and applications.**

measures such as limitations on their use, e.g., "sensing" by RFID readers is done only when airplanes are on the ground.[13] However, for addressing security concerns it is pivotal to understand and mitigate threats to the eEnabled airplane and its applications. Therefore, this paper considers the security of the AANET.

The remainder of this paper is as follows. Section II describes the network and adversary model considered, as well as major threats to the assets of the AANET. Section III presents the proposed security requirements and mitigation solutions. Section IV discusses some of the major challenges and open problems in securing the AANET. Section V covers some of the related research and standards. Section VI concludes the paper.

## II. eEnabled Aircraft Ad hoc Network Model

Fig. 1 illustrates a generic AANET model considered in this paper. Communications between the eEnabled airplane and the airline infrastructure can occur either over a broadband satellite link when the airplane is in-the-air (e.g., INMARSAT[3]) or a 802.1x based link when on-the-ground (e.g., Gatelink[24] at the airport terminal). With the air traffic controllers, aeronautical-specific communication protocols (e.g., ACARS[3]) are used over a satellite link or a terrestrial link based on VHF/HF[3] or 1090 MHz Extended Squitter (1090-ES).[26] Further, communications between airplanes can occur over the UHF radio link provided by ADS-B. Furthermore, in the future, it can be anticipated that the eEnabled airplane may also communicate over 802.1x-based broadband links with unmanned aerial systems for services from third party providers.

These wireless channels are used to communicate *information assets* between airplanes or airplanes and the ground infrastructure at the airlines, air traffic controllers, and third party service providers. We consider the information assets to include loadable software specified in RTCA DO-178B (e.g., avionics software, navigation databases), flight bag,[28] traffic beacons or information (e.g., airplane locations or real-time weather),[34] health diagnostics and prognostics of aircraft structures or systems,[24] and in-flight entertainment content.[3]

The eEnabled airplane has onboard wired/wireless sensors, RFID tags and readers deployed on structures and systems, providing feedback for diagnostics and prognostics in health management.[10,24] Further, it has an onboard ADS-B unit using GPS to compute and update airplane locations and broadcast them as beacons for use in traffic management tasks, such as surveillance and navigation.[34] ADS-B can also receive beacons from other airplanes as well as information broadcasts from ground controllers, e.g., real-time weather or locations of airplanes that do not have ADS-B. Furthermore, airline systems can deliver assets to onboard line replacable units, such as loadable software, flight bag, or in-flight entertainment, as well as initiate a download of assets from onboard systems, such as health diagnostics or configuration reports.[22]

### A. AANET Assumptions

Access to the AANET is assumed to be managed properly. It is also assumed that cryptographic and security quantities are properly managed and protected. Sufficient protection is provided in the AANET for robustness against well known denial of service attacks. In case of a network systems failure, asset distribution via physical media is assumed adequate to meet requirements for timely data delivery from an aircraft in some applications, such as for delivery of software or download of health data. Further, airlines are assumed capable of managing configurations and health of their fleet in a reliable and correct manner. Sufficient physical security checks are in place to prevent unauthorized cabin access to onboard systems. Additionally, the air traffic controllers are assumed to properly conduct the traffic management tasks. Third party service providers are not considered responsible for airplane operation.

### B. AANET Constraints

Any solution approach for the AANET, must account for the following constraints of the eEnabled airplane.

**Regulatory Constraints.** Regulatory agencies provide certain mandatory guidelines that must be met for the airplane to be considered airworthy and flight-ready. As a result, any new mechanism or requirement from the AANET must be integrable with the existing well-defined regulations.

**Time Constraints.** Average lifetime of a typical commercial plane, and hence of its assets, is in the order of several decades. Time-dependent requirements for the airplane assets must take this constraint into account. The constraint also imposes the need for long-term solutions. Further, the different phases of flight can be categorized into three operational stages: on-the-ground, takeoff or landing, and in-flight. The time period of each operational stage of the airplane is fixed. Applications and mechanisms are therefore expected to function within these time constraints. Furthermore, some real-time operations of the airplane must be performed in a timely manner requiring computation and communication efficient solutions.

**End-to-End Trajectory Constraints.** In its end-to-end flight, an airplane may traverse multiple airports with possible lack of network connectivity at one or more traversed airports. Additionally, the airplane may find varying network environment such as in terms of protocol standards, security technologies, export restrictions.[24] The airplane may also interact with multiple off-board systems, e.g., airport wireless access point and airline systems. Solutions for the AANET therefore must be adaptable and scalable to ensure seamless air travel for the airplane. Furthermore, airplanes follow predictable routes, except during Free Flight,[25] and travel from airport to airport in an estimated trip time. Therefore, airplanes within communication range and moving in a similar direction can be expected to navigate as a group of nodes forming a fully connected network graph within the group. For example, ADS-B based on 1090-ES can provide a communication range between 40 to 90 nautical miles.[26]

**Airlines Cost Constraints.** The airline fleet operation and maintenance costs must be reduced. Therefore, any proposed solution for the AANET must minimize overhead at the airlines. Further, in order to obtain return-of-investment from existing systems and processes, any new technology must be compatible with legacy systems and processes in commercial aviation.[24]

### C. Adversary Model Considered

Wireless technologies provide easy open access to RF communications. For example, the proposed onboard use of transmitting personal electronic devices which can include laptops, RFID tags and cell phones,[19] raises a potential vulnerability for disruption or unauthorized access to wireless communications of the eEnabled airplane. Therefore, an adversary can perform remote attacks in the AANET to manipulate airplane operation and availability in unexpected ways.

The overall objective of the adversarial attacks considered is to impede beneficial operation of the e-enabled airplane by attacking its information assets, e.g., motivation of hackers or criminal organizations. The adversary can be external to the AANET and/or an insider. For simplifying analysis, we consider attacks to be

only over wireless links in the AANET. The adversary is capable of passive attacks such as network traffic analysis, as well as active attacks such as node impersonation attack, and compromise of unattended sensors, tags, readers, or ADS-B ground controllers. It is also assumed that the adversary is capable of jamming the wireless channels.

We note that insider attacks based on compromised sensors, tags or readers can be deterred by enforcing legal regulations and sufficiently safeguarded against with specific physical, logical and organizational inhibitors, checks and control. 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 onboard systems.

### D. Security Threats to AANET

**Corruption of Assets.** The adversary may attempt to corrupt certain critical assets in the AANET to create safety concerns from an evident degradation of airplane airworthiness, or induce business concerns from false alarms and late detection of corruption leading to unwarranted flight delays and costs. Some examples for critical assets include loadable software at RTCA DO-178B Level A-E or flight bag used in flight operation and management, software configuration reports used to decide flight readiness, health diagnostics used to detect/monitor faults, and traffic beacons which are used to determine flight trajectory options.

**Misuse of Assets.** Assets may include information useful for the adversary in sidechannel attacks, e.g., airplane locations or fuel levels. Certain assets may also be considered to be intellectual property with business value, e.g., RFID tag data which may contain some sensitive part maintenance data.

**Liability.** Any entity in the AANET could deny having performed some security-relevant action on assets after detection of their manipulation.

**Delay of Assets.** Assets can be made inaccessible by jamming wireless channels to disrupt applications.

## III. Securing the AANET

### A. Basic Security Requirements

**Integrity and Authenticity** For preventing any corruption of 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 source. Further, the source identity must also be verified.

**Authorization** The verifiable identity of each entity accessing or distributing any asset in the AANET, must be checked to possess the appropriate permission and privilege.

**Confidentiality** Unauthorized access to sensitive assets that can be leveraged for future attacks or personal gain must be prevented.

**Early and Correct Detection** Any manipulation of an asset must be detected as soon as possible so as to not disrupt the predicted time for flight discussed in Section II.B, while also eliminating or reducing false alarms.

**Availability** Each asset must be available soon enough to meet the airplane time constraints discussed in Section II.B.

**Traceability and Non-repudiation** 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. Further, for the purpose of forensics, the traceability of actions on each asset must be undeniably associated with at least one authorized entity.

**Table 1. Mapping of security threats and requirements using digital signatures as a mitigation solution. $\surd$ – satisfied; $C$ – partially satisfied; $\times$ – not satisfied.**

| **Requirement/Threat** | Corruption of Assets | Misuse of Assets | Liability | Delay of Assets |
|---|---|---|---|---|
| Integrity & Authenticity | $C$ | $\times$ | $\surd$ | $\times$ |
| Authorization | $C$ | $\times$ | $\times$ | $\times$ |
| Confidentiality | $\times$ | $\surd$ | $\times$ | $\times$ |
| Early & Correct Detection | $C$ | $\times$ | $\times$ | $\times$ |
| Availability | $\times$ | $\times$ | $\times$ | $C$ |
| Traceability | $C$ | $\times$ | $\surd$ | $\times$ |
| Non-repudiation | $\times$ | $\times$ | $\surd$ | $\times$ |

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

### B. Digital Signature as a Solution Building Block

Digital signatures offer an attractive mechanism to secure assets in the AANET. A generic signed asset from a source to a destination in the AANET will be of the form:

$$asset, sign_{source}(H(asset), timestamp), certificate_{source}$$

where $sign_x(.)$ denotes signature of an entity $x$ and $H(.)$ is a one-way cryptographic hash. $a, b$ denotes concatenation of two strings $a$ and $b$.

In order to verify the signature, a valid certificate of the source is needed:

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

where the CA is the Certificate Authority, a trusted third party. The source certificate can be validated using the CA's valid public key and checking the validity period. Therefore, assuming the CA's public key is known, the destination can use $cert_{source}$ and $tstamp$ to verify the *integrity* and *authenticity* of the received asset. Verifying signatures as soon as it received can contribute to the *early and correct detection* of corrupted assets. Signatures in combination with audit logs are sufficient for achieving *non-repudiation* and *traceability*. Further, use of digital signatures allows the use of asymmetric key encryption for *confidentiality*. Moreover, for scenarios where the AANET communications are subject to stringent delay constraints, symmetric key cryptography can provide more efficient solutions for integrity and confidentiality, such as Secure Socket Layer (SSL).[3]

Table 1 shows which threats can be mitigated using the above solution mechanisms for meeting security requirements. As shown in Table 1, the delay and corruption of assets is only conditionally covered. This is because the AANET is still susceptible to jamming and sidechannel attacks by the adversary, respectively. We cover mitigation of these attacks in the next section.

### C. Mitigation of Jamming and Sidechannel Attacks

**Wireless Channel Jamming.** While availability in the AANET can be achieved with host and network protection mechanisms,[3] separate mechanisms are needed to detect and mitigate wireless jamming attacks. Leveraging the broadcast medium of wireless channels, the adversary can employ jamming attacks to block or delay communications, e.g., from airplane to ground or even from onboard sensors and RFID tags to airplane subsystems. Therefore, channel jamming attacks must be detected as soon as possible and mitigated in the AANET. The detection and defense of jamming attacks launched in different layers of network is an active research area, and interested readers are referred to[15] for an overview of recent research advances in this area.

**Table 2. AANET constraints and implications for use of digital signatures.**

| Constraint | Implications for Digital Signatures |
|---|---|
| Regulatory constraints | Guidelines for key and certificate management |
| Time constraints | Long-term security solutions<br>Efficient signature schemes |
| End-to-end trajectory constraints | Emerging challenges for PKI<br>Scaleable offline verification mechanisms |
| Airline cost constraints | Key and certificate management processes |

**Routing Vulnerabilities.** For enhancing information reachability to remote areas, airplanes can form a multi-hop route.[26] Further, onboard sensors may also form multi-hop communication routes to conserve energy.[10] Nodes is these routes must forward data in a timely and reliably manner, even under attacks. Therefore, the routing protocols employed in the AANET must be robust to jamming attacks that induce long and energy-inefficient routes as well as to attacks based on misleading routing messages. For example, if geographic routing is used then by spoofing location information (e.g., the wormhole attack[16,30]) a compromised node can modify routes as desired by it.

**Software Vulnerabilities.** Each airplane model has a specific loadable software configuration. Further, different versions of loadable software for an airplane model may incompatible. The adversary can attempt to exploit these vulnerabilities and prevent distribution of signed software updates to an airplane or divert signed software to an unintended airplane model, resulting in detectable anomalies. A mitigation approach is to include version number and intended destination of the software in its signature metadata.

**Location Dependency.** Sensor readings and traffic beacons must include locations to be useful. Further, network services, such as geographic routing, require location information of nodes. The adversary may leverage this dependency on location in the AANET for attacks, e.g., by spoofing locations or corrupting location data. Hence, nodes must be capable of securely verifying the location claims made by their neighbors[16,36] and also including accuracy of location data in the signed traffic beacons.[34] Secure location verification also provides another level of source authenticity using the position of a neighbor to verify validity of data received from it. Furthermore, the location of some sensors or airplanes can be sensitive due to their due to their value for launching other attacks. In such scenarios, the AANET communications must not reveal node locations and type to unauthorized entities.

**Node Capture/Compromise.** For addressing insider attacks based on compromised nodes in the AANET, tamper-proof hardware offers one potential solution. However, since this solution can be expensive and not scalable, the design of algorithms for all the above primitives must be capable of tolerating compromise of a fraction of network nodes.[17]

### D. Impact of AANET Constraints on Digital Signatures

Table 2 summarizes some of the major implications for the AANET with the use of digital signatures and in the presence of the constraints discussed in Section II.B. As shown, the airplane time constraints impose that a careful consideration be given to the potential for key compromise. Increase in cryptanalytic capabilities available to the adversary over time can also increase the potential for compromise of the signing key of the source. Therefore, in order to extend the lifetime of asset signatures in AANET, mechanisms such as periodic key refresh, longer keys or provably secure/forward secure signature algorithms need to be employed.

Further, the airplane end-to-end trajectory constraints impose restrictions on the mechanisms employed to verify signatures. Digital signatures usually require a Public Key Infrastructure (PKI), i.e., a mechanism for managing identities with associated keys and certificates in the AANET.[23] However, use of a 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.[8] Moreover, as seen later in Section IV.C, evaluating a complex system such as PKI at an adequate assurance level for the AANET can be a major challenge as well. Further, offline mechanisms, such as use of pre-loaded certificates, is needed to compensate for any lack of connectivity at a traversed airport. However, this choice is complicated by the need for scalability in the AANET.

Furthermore, in order to satisfy regulatory and airlines cost constraints, proper certificate and key management processes must be defined. Regulatory agencies understand that the introduction of digital certificates and cryptographic keys in onboard system storage clearly affects existing guidance for airplanes. Airlines that currently do not fully support any PKI may need guidelines to cover the corresponding requirements for updating and distributing keys and certificates.

## IV. Challenges and Open Problems

This section discusses some of the major security challenges and problems in the AANET.

### A. Impact of 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.[21,37] For instance, cooperative navigation and collision avoidance applications in VANET have the same objective as their counterparts in the airborne ad hoc networks. Further, group navigation, discussed in Section II.B, is a common property of both networks.[37] Interesting research may lie in leveraging design of secure solutions being developed in VANET, for mitigating threats to AANET. For example, the position information broadcasts from airplanes approaching or navigating in an urban environment, such as terminal areas, can potentially present sidechannel information for unauthorized parties. In such scenarios, it may be useful to employ anonymous identifiers and mitigation of unauthorized location tracking in airborne ad hoc networks.[37]

### B. Impact of Security on Safety

Although existing literature argue for commonality among the safety and security disciplines,[38,39] 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.[24] 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.[5]

### C. PKI and Formal Methods for High Assurance of AANET Applications

A security analysis of the distribution of loadable software for eEnabled airplanes, shows that it is desirable to evaluate application supporting systems at a high assurance level. However, this presents two main problems that still remain to be resolved. One, the maximum assurance level of commercially available PKI is currently limited to medium assurance levels. Consequently, for evaluation of AANET applications using digital signatures at a high assurance level, it is necessary to first design and implement a PKI at that level.[5] Two, high assurance evaluation requires consideration for the use of complex analytical tools, such as formal methods. The use of formal methods can be time consuming and expensive, giving rise to challenges from airline cost constraints.[5]

### D. Impact of Wireless Technologies on Airworthiness

Guidelines for certified use of passive-only RFID tags onboard commercial airplanes has been developed.[13] 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. Nevertheless, any future approval of active RFID tags for onboard use would provide a stepping stone for the use of the wireless sensors as well.

### E. Real-Time Networked Control System Design

Most of the current approaches analyzing the stability of networked control systems consider delays[20] and packet losses[33] 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,[20] 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.

## V. Related Work

In this section, we overview some of the major standards and recent research related to security of the eEnabled airplane.

### A. Developing Standards

Major standards in the networking and security have been developed or are emerging for the eEnabled airplane. ARINC 664 introduced commercial ethernet standards for the aircraft network and recommended an architecture that securely separates the flight critical systems from others. ARINC 811 improves this architecture and proposes a security framework to identify potential mechanisms to protect the in-aircraft network while taking into account the needs and constraints of airlines. ARINC 666 is currently in development to define the format of electronic delivery of loadable software over networks. Specifically, it defines the crate format that contains the signed software parts and other information. RTCA D0-178B is a well-established guidance for equipment suppliers to design and develop loadable software for their onboard equipment. It defines five levels for loadable software based on their failure impact on flight safety, i.e., Level A to Level E, with decreasing safety criticality and associated certification effort; RTCA DO-178C will additionally account for the use of formal methods for verifying loadable software properties. RTCA Special Committee SC-202 is considering the interference from transmitting personal electronic devices onboard (e.g., cellular devices, active RFID tags, embedded medical sensors), 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. For security and privacy of the RFID tag data it currently recommends use of password based mechanisms. RTCA SC-186 has taken on the role of standardizing the ADS-B and its commercial aviation implementations based on 1090-ES data link. A variety of applications based on the ADS-B A2I/A2A beacons is identified in RTCA DO-242A. Furthermore, RTCA SC-203 is currently leading the initiative of safely introducing UASs in the national airspace for civilian applications.

### B. Ongoing Research

Research efforts in the security of commercial aviation focus on emerging applications and issues currently not addressed by the standards. For example, an evaluation of different security mechanisms that can strengthen aircraft network architecture is presented.[3,24,28] A standardized security framework based on the Common Criteria methodology has been proposed to analyze a generic system for electronic distribution of loadable software.[5,22] Secure integration of potential onboard wireless technologies are also being considered, such as use of wireless sensor networks and RFID tags for airplane health monitoring.[9,10] Further, the anticipated impact of unprecedented requirements arising from the use of security solutions on the commercial aviation

information systems and processes are being identified.[23] Furthermore, vulnerabilities in ADS-B based surveillance applications are being studied.[36]

## VI. Conclusions

In this paper, we studied the security of an eEnabled airplane ad hoc network (AANET) that can emerge in the future. The AANET promises applications that can significantly benefit next-generation air transportation systems. Our security analysis focused on information assets that could impact airplane operation, airplane maintenance and air traffic control, and provided a classification for major threats to the AANET. We proposed digital signatures as a basic solution approach and presented some of the challenges that can be expected with their use in the AANET. Further, sidechannel attacks that were not addressed by signatures were also considered. A major security-related task with wide deployment of AANET is the high confidence evaluation of the its applications. Our work on the assurance of electronic distribution of airplane loadable software takes a step towards this direction.

## References


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

[2]Advisory Council for Aeronautics Research in Europe. www.acare4europe.org/

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

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

[5]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.

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

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

[8]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.

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

[10]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.

[11]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

[12]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

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

[14]Common Criteria. http://www.commoncriteriaportal.org/

[15]Li, M., Koutsopoulos, I., Poovendran, R., Optimal jamming attacks and network defense policies in wireless sensor networks, *Proceedings of IEEE INFOCOM*, 2007, pp. 1307-1315.

[16]Lazos, L. and Poovendran, R., SeRLoc: Robust localization for wireless sensor networks, *ACM Transactions on Sensor Networks*, Vol. 1, No. 1, 2005, pp. 73-100.

[17]Tague, P. and Poovendran, R., A canonical seed assignment model for key predistribution in wireless sensor networks, *ACM Transactions on Sensor Networks,* 2007.

[18]Lazos, L. and Poovendran, R., Power proximity based key management for secure multicast in ad hoc networks, *ACM Journal on Wireless Networks (WINET)*, Vol. 13, No. 1, 2007, pp. 127-148.

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

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

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

[22]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.

[23]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.

[24]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.

[25]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.

[26]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.

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

[30]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.

[31]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.

[32]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.

[33]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.

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

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

[36]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.

[37]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.

[38]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.

[39]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.