Networked CPS View of a Future Airspace

Krishna Sampigethaya[1], Sudhakar Shetty[1], Terry Davis[1], Mingyan Li[1],
Scott Lintelman[1], Richard Robinson[1], Linda Bushnell[2]
[1] The Boeing Company, Seattle, WA, USA
[2] University of Washington, Seattle, WA, USA
{radhakrishna.sampigethaya,sudhakar.shetty,terry.l.davis,scott.lintelman,mingyan.li,
richard.v.robinson}@boeing.com, lb2@u.washington.edu

Abstract— **This paper considers a future airspace shared by operational manned and unmanned air vehicles digitally linked with each other and with ground infrastructure, as a large-scale, dynamic cyber-physical system. Such a CPS must exhibit deterministic and adaptive behavior, as well as meet real-time performance requirements. The comprehensive goal of enhancing safety, security, reliability, efficiency, capacity and usability of an automated, decentralized airspace, leads to some unique challenges and open problems. We expect that advanced research in CPS can mutually benefit next-generation airspace and intelligent roads.**

I. INTRODUCTION

Aviation has become a major driver of global economy, with passenger and cargo traffic reaching unprecedented levels during the last decade. Crowded skies combined passenger and airline needs, as well as growing concerns about environmental footprint of aviation, have however overwhelmed the current capacity and capabilities of air transportation infrastructure. Today, technologies, applications and processes are being introduced to enhance airspace capacity as well as aspects of airplane operation, control, and maintenance [1][2].

The "e-enabled airplane" is envisioned to be an intelligent node with advanced computing technologies such as GPS, RFID and wireless sensors, seamlessly traversing a global information network [3]. The expected enhancements in information delivery, availability, usage and management promise cost-effective improvements in the next-generation air transportation systems. As shown in Fig. 1, A2I (aircraft-to-infrastructure) and A2A (aircraft-to-aircraft) communications allow airplanes to form an *airborne ad hoc network* that can enhance information sharing and situational awareness of airplanes. This capability can be key to improve the current in-efficient and highly centralized air traffic management, as well as the current delayed and error-prone integrated vehicle health management system. Automating and sharing traffic control tasks between airplane and ground controllers, e.g., aircraft safe separation and weather prediction, can enhance airborne navigation and ground air traffic surveillance [4]. Real-time sensing and sharing of onboard health diagnostics with aerospace engineers and equipment suppliers can enable synchronized and proactive airplane maintenance [2]. The world-wide deployment of enabling infrastructures, e.g., Asynchronous Dependent Surveillance Broadcast (ADS-B) and 1090 MHz Extended Squitter data links for A2A/A2I communication range of 40–90 nautical miles, support the future of airborne ad hoc networks [5].

However, with off-the-shelf solutions and open networked systems onboard, new vulnerabilities are introduced to create potential airworthiness concerns and airline business disruptions. Current regulatory guidance and regulations for continued airworthiness are only beginning to cover security threats to the e-enabled airplane onboard systems and information assets [6]. Before e-enabled commercial, military and general aviation aircraft as well as unmanned aircraft systems share the national airspace, major safety and security concerns with airborne ad hoc networks must be identified and mitigated. To address such concerns and build trustworthiness in the e-enabled airplane operation, control and maintenance, this paper models the airspace as a safety and security-critical aviation *cyber-physical system* (CPS).

II. AVIATION CPS MODEL

Fig. 1 shows an abstraction of the e-enabled airplane system-of-systems using advanced wireless technologies for delivery of time- and safety-critical air traffic and airplane health assets, i.e., traffic beacons and critical diagnostics/prognostics, as well as delay-tolerant but business-critical traffic and health data.

From a CPS viewpoint, each airplane represents a sensory system composed of collaborating onboard sensors and RFID infrastructure, an actuator system composed of networked onboard actuators, and an onboard controller which receives sensing feedback and sends actuations. The airplanes can collaborate to form a dynamic multi-layered sensing system which monitors their internal and surrounding environments, as well as a dynamic multi-layered actuator system which controls their physical behaviors. Both systems are data linked to the cyber-world by the ground stations owned or operated by different entities such as airports, traffic controllers, airlines, etc.

Any findings, conclusions or recommendations in this material are those of the authors, and should not be interpreted as of The Boeing Company. We thank Prof. Radha Poovendran from the Network Security Lab at University of Washington for his valuable contributions to this work.

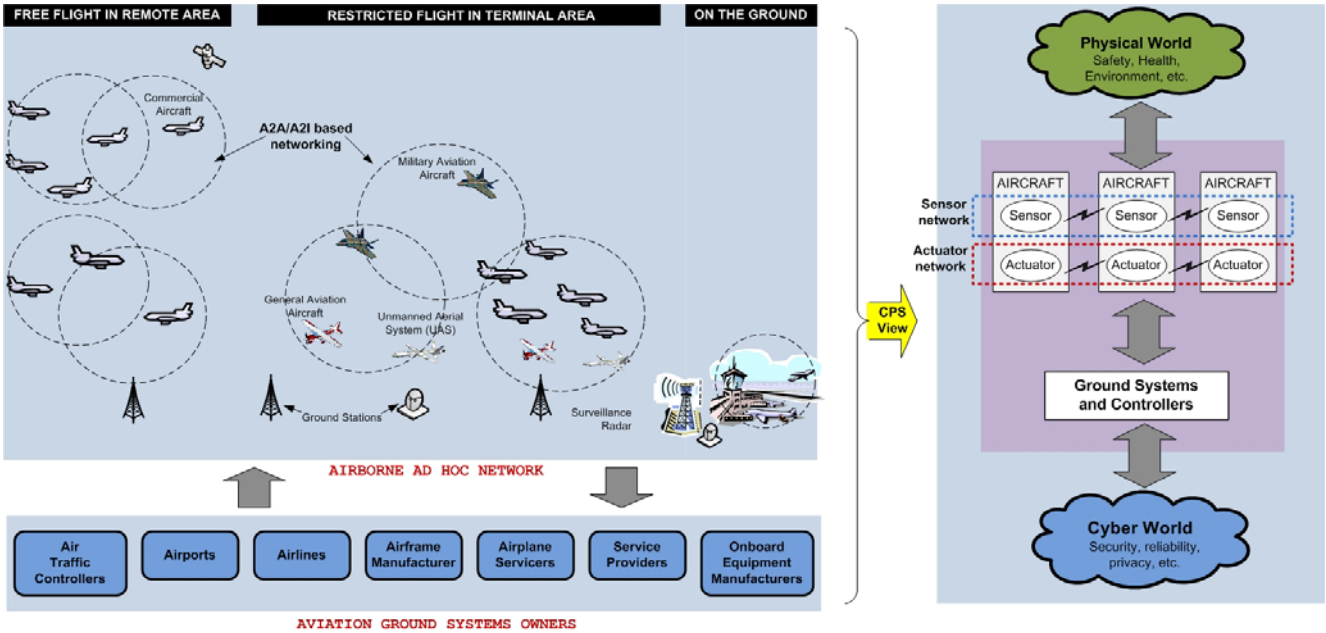
FREE FLIGHT IN REMOTE AREA
RESTRICTED FLIGHT IN TERMINAL AREA
ON THE GROUND
Commercial Aircraft
A2A/A2I based networking
Military Aviation Aircraft
General Aviation Aircraft
Unmanned Aerial System (UAS)
Ground Stations
Surveillance Radar
AIRBORNE AD HOC NETWORK
Air Traffic Controllers
Airports
Airlines
Airframe Manufacturer
Airplane Servicers
Service Providers
Onboard Equipment Manufacturers
AVIATION GROUND SYSTEMS OWNERS
CPS View
Physical World
Safety, Health, Environment, etc.
Sensor network
Actuator network
AIRCRAFT
Sensor
Actuator
Ground Systems and Controllers
Cyber World
Security, reliability, privacy, etc.

Fig. 1: Illustration of a CPS model of a future airspace shared by networked air vehicles, and the asset flow.

This aviation CPS is a large-scale distributed control system, comprised of diverse interacting groups of mobile agents (i.e., air vehicles) that can establish structured hierarchies based on their capabilities. The airborne ad hoc network consists of the *control network* (e.g., using ADS-B data links) and *monitoring network* (e.g., using terrestrial or SATCOM links). To prevent unwanted and malicious control responses, the CPS must protect communications and prevent unauthorized access, maintaining reliability in the presence of faults and adversarial attacks in the airborne ad hoc network. Further, to be deployable, reliability must be guaranteed with superior performance in terms of real-time operations. We present some of the major research problems that emerge from this CPS model.

III. Major Research Problems in Aviation CPS

Secure Distribution of CPS Assets. Corruption of safety-critical data, e.g., ADS-In beacons, structural damage diagnostics, can be potentially lower target airplane(s) airworthiness, while tampering of non-safety-critical data, e.g., detection of a failing cabin temperature sensor, may disrupt businesses operating in the nation’s passenger and cargo transport infrastructure. Therefore, end-to-end integrity and authenticity must be guaranteed in data distribution in the airborne network. A potential solution approach is to leverage an IA solution that we have developed to distribute airplane assets such as loadable software, flight bag, and software configuration reports [7]. For instance, this solution can be extended to assure integrity and authenticity between the airplane and end-user of the data on the ground, e.g., onboard equipment suppliers who will receive real-time part/equipment diagnostics or status from airlines in next-generation integrated vehicle health management.

Secure and Reliable Control Network. Attacks on the control data (e.g., ADS-B beacon) integrity and protocols can compromise critical control network functionality. Therefore, the major class of threats must be identified, along with modeling of the attacks to evaluate the impact of attacks on airplane behavior. Further, for end-to-end data integrity, efficient asymmetric- and symmetric-key-based authentication mechanisms which satisfy time-critical constraints, must be developed.

Performance of Secure Wireless Networked Control. The control network will be used by air vehicles in the shared airspace and additionally be used for distribution of large volumes of potentially non-safety critical data, e.g., traffic information and updates from ground systems. The control network must however exhibit determinism for time-critical operations, e.g., in terms of end-to-end delay and packet delivery rate. Hence the performance of mechanisms for secure wireless networked control of non-safety and safety-critical operations under mixed network traffic loads and air traffic density must be studied.

Securing Physical Links and Devices. The airborne ad hoc network is mainly characterized by the physical links and networked devices. Unlike traditional networks that emphasize only on data confidentiality, integrity and end-to-end transfer, the airborne network must address security and reliability aspects at the physical layer as well, i.e., require the design of cross-layer solutions.

Further, a major challenge is to correctly characterize the radio environment of airborne networks, and design lower-layer enforcement strategies exploiting unique features of the multipath channel for securing the physical links. Furthermore, trusted computing techniques are needed to enforce deterministic behavior from the networked onboard controllers, sensing and actuator systems on airplanes. The incorporated technologies will enable assessment of trust level locally and remotely.

Policy Enforcement. A standard global policy specifying correct interactions between the airborne ad hoc network nodes, i.e., between airplanes as well as between airplanes and airports, must be designed. Apart from policy specification, the policy must be enforced to prevent violation by a compromised onboard or ground controller. A major weakness with the use of a centralized solution for enforcing policy among the control network nodes, is the risk of creating a single point of failure. Hence, a distributed policy enforcement technique is needed to regulate the behavior of the mobile airplanes.

IV. Practical Challenges

We present some of the major challenges in the design, development and deployment of the aviation CPS.

Providing key and certificate management – The use of digital signatures imposes the need to integrate mechanisms and processes that can manage keys and certificates. However, factors such as global traversed paths of airplane, lack of guaranteed seamless network connectivity, multiple connecting ground stations and applications, lifetime of CPS assets, and airline cost constraints, complicate the design of suitable solutions for managing airplane private keys as well as certificates for validating received assets and airborne/ground entities.

Additionally, the use of a PKI to support digital signatures requires interoperability between multiple Certificate Authorities and the standardization of a certificate policy for aviation to enable global seamless air travel Furthermore, PKI can also limit the achievable assurance level of the system using it.

Achieving high assurance for a complex system – To enable the beneficial and secure use of a system for CPS asset distribution, high confidence in the end-to-end security properties is needed. However, system-of-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 CPS. 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 CPS components.

Analyzing impact of security on safety – While it is clear that security affects safety, it is not clear how to present security requirements and functions in the context of a safety analysis. Since impact of security threats can evolve, the traditional quantitative and probabilistic safety analysis techniques become inapplicable for security evaluation. Therefore, new approaches are needed to integrate the discrete security evaluation methods into safety analysis.

V. Relevance to Automotive CPS

While the traversed paths of vehicles do not scale globally, the number of deployed vehicles is relatively large. This scalability requirement presents unique PKI challenges, including key and certificate management. Moreover, certificate management is further complicated by change of ownership which can be expected to be more frequent for automotive CPS. Both sectors share applications that have functional similarities, such as collision avoidance and cooperative driving in vehicular networks [8] compared to conflict detection /resolution and other free flight tasks in airborne ad hoc networks. Therefore, one of our future focuses is to identify technology and application areas where both aviation and automotive sector find common benefit from advanced research and development.

References

[1] G. Bird, M. Christensen, D. Lutz, and P. Scandura, “Use of integrated vehicle health management in the field of commercial aviation,” Proc. of NASA ISHEM Forum, 2005.

[2] S. Shetty, “System of systems design for worldwide commercial aircraft networks,” Proc. of ICAS, 2008.

[3] C. Wargo and C. Dhas, “Security considerations for the e-enabled aircraft,” Proc. of Aerospace Conference, 2003.

[4] G. Pappas, C. Tomlin, J. Lygeros, D. Godbole, and S. Sastry, “A next generation architecture for air traffic management systems,” Proc. of IEEE conference on Decision and Control, pp. 2405–2410, 1997.

[5] J. Krozel and I. Andrisani, “Independent ADS-B Verification and Validation,” Proc. of AIAA ATIO, pp. 1–11, 2005.

[6] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security—Protection of Airplane Systems and Data Networks From Unauthorized External Access, [Docket No. NM365 Special Conditions No. 25–07–02–SC], Federal Register, Vol. 72, No. 72, 2007.

[7] 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,” SAFECOMP, 2007.

[8] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET,” IEEE JSAC, 25:8, p. 1569, 2007.

Scott Lintelman is the Information Assurance (IA) manager at Boeing Networked Systems Technology, responsible for setting Boeing’s IA research strategy. *Krishna Sampigethaya*, *Mingyan Li* and *Richard Robinson* lead the security effort of the Boeing Phantom Works IA group. *Sudhakar Shetty* and *Terry Davis* are IA researchers and leads in the Boeing Commercial Airplanes. The IA team has a long-standing partnership with BCA. *Linda Bushnell* is a Research Assistant Professor in the EE department at the University of Washington and director of the Networked Control Systems Lab.