SECURE WIRELESS COLLECTION AND DISTRIBUTION OF COMMERCIAL AIRPLANE HEALTH DATA

Krishna Sampigethaya[*]*, Mingyan Li*[†]*, Radha Poovendran*[*]*, Richard Robinson*[†]*,*
Linda Bushnell[*]*, Scott Lintelman*[†]
[*] *Department of Electrical Engineering, University of Washington, Seattle, WA*
[†] *Boeing Phantom Works, Bellevue, WA*

Abstract

The introduction of wireless communication capabilities supporting transfer of sensor data and information on board commercial airplanes as well as between airplanes and supporting ground systems has the potential to significantly improve the safety and efficiency of air travel. The benefits, however, come at the cost of information security vulnerabilities introduced by data networks. Regulatory institutions, including the FAA, are aware that security requirements for network-enabled airplanes must be fully identified. Therefore, this paper focuses on wireless airplane health monitoring and management, and contributes a security framework to identify threats and system requirements to mitigate these threats. We also present challenges and open problems in enabling secure use of wireless sensor networks for health monitoring and control of commercial airplanes.

Introduction

Commercial aviation is at the threshold of a new era, that of an “eEnabled” airplane equipped with wired and wireless networking capabilities and significant onboard information processing and storage resources. The eEnabled airplanes represent an exciting future-directed development in the avionics industry. Participating as a node in an air transport business’s information technology (IT) infrastructure, the eEnabled airplane affords capabilities to facilitate a broad spectrum of new beneficial network-based applications, including electronic distribution of field-loadable software and electronic “flight bag” information from ground-based systems, collection of health data by onboard wireless sensors, and health data distribution to ground systems.

This paper focuses on one specific future application, i.e. the health monitoring and management of eEnabled airplanes which allows the transition from current fixed-interval scheduled maintenance to future automated, real-time and continuous inspection of airplanes. The FAA has envisioned health monitoring and management as a future maintenance technology and a key enabler for next-generation airplanes, such as Boeing 787 and Airbus A380 models [1]. The airplane health monitoring and management system or AHMMS, continually monitors health of airplane structures and systems via embedded sensors, providing timely feedback to onboard units (e.g. flight control computer) and off-board units (e.g. airline ground server) for health assessment. As shown in Fig. 1, the feedback can be used by onboard controllers for real-time operation or by ground controllers for proactively monitoring the airplane systems status. Consequently, the AHMMS can significantly improve efficiency and effectiveness of scheduled maintenance process for commercial airplanes [1].

The benefits of eEnabled airplane applications, however, cannot be realized without giving rigorous consideration to the security requirements for addressing the vulnerabilities introduced with the use of open networks and commercial-off-the-shelf IT components [5]. The regulatory agencies, including the FAA, are aware of this unprecedented need for airplane network security requirements; existing guidelines for airworthiness do not incorporate the requirements to thwart the network security threats [6] [7].

In this paper, we consider the use of wireless sensor networks (WSNs) for the health monitoring functionality of the AHMMS. Today, WSNs are revolutionizing data collection capabilities. The AHMMS presents an opportunity for the avionics industry to benefit from WSN as other industries are beginning to realize. The use of WSNs offers advantages, such as significant reduction of system weight and onboard wiring costs [2] [3] [4]. Further, wireless sensors can be deployed and

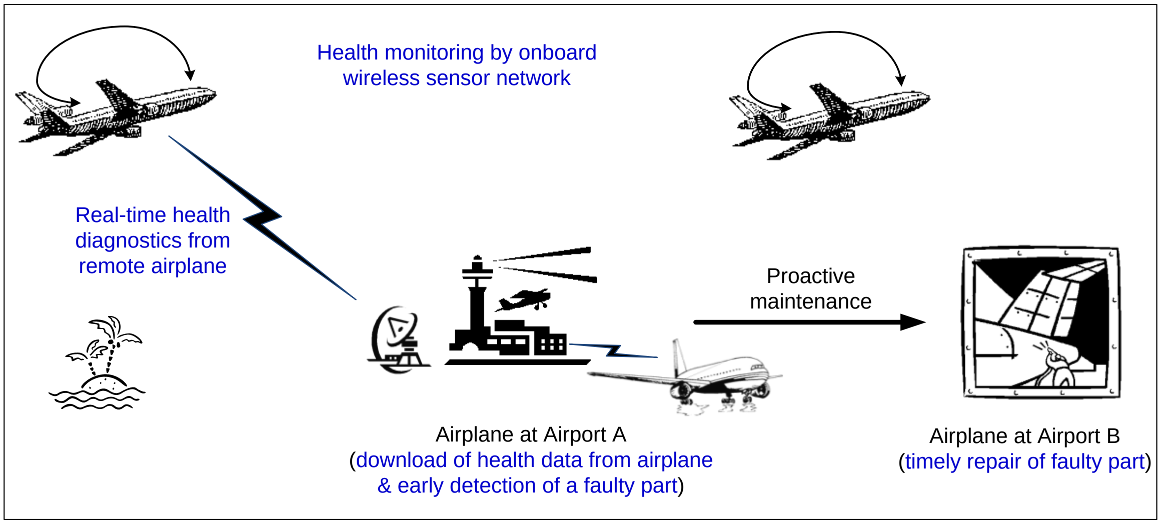
Health monitoring by onboard wireless sensor network
Real-time health diagnostics from remote airplane
Proactive maintenance
Airplane at Airport A
(download of health data from airplane & early detection of a faulty part)
Airplane at Airport B
(timely repair of faulty part)

Figure 1. Illustration of the AHMMS functionalities.

networked when needed, avoiding expensive redesign of wiring layouts. Additionally, wireless links can be more tolerant in the presence of harsh conditions such as high temperature [3]. As a result, cost-effectiveness, reliability and safety of AHMMS technology can be improved by WSN.

In the case of the AHMMS, the ease of accessibility to wireless communications provides windows for unauthorized, remote access and new opportunities for attackers to manipulate the health data without physically accessing the onboard sensors and other avionics systems. New security threats to the airplane safety and business of airplane operators emerge. For example, a malicious attacker may manipulate monitoring data (e.g. engine health data) to hide sensor detected safety-critical issues that may warrant real-time actions, therefore lowering the airplane's safety-margin. On the other hand, data manipulation can raise false alarm to incur unwarranted airplane maintenance costs, impeding business operations. Further, certain onboard sensor readings and WSN communications (e.g. related to fuel level) can be considered sensitive because of their potential use for future attacks. Therefore, it is pivotal to understand the security threats to the data collection by the WSN as well as data distribution to the ground systems in the AHMMS.

The main contribution of this paper is our ongoing investigation into the secure use of WSNs in AHMMS. To the best of our knowledge, this paper is the first work to address the security of WSNs used to sense and collect data for AHMMS. Additionally, the paper leverages our prior work on secure electronic distribution of software and data between airplane and ground systems [8] [9], in which a Common Criteria (CC) [10] standard-based framework is proposed to identify specific security threats, requirements, and mitigation mechanisms. Thus, this paper presents a security solution for end-to-end distribution of health data.

In the next section, we present the AHMMS system model and the types of adversarial attacks considered, followed by a classification of the resulting security threats to health data collection and distribution. We then propose security requirements for the AHMMS, and discuss challenges in related avionics that must be addressed to enable the use of secure solutions. Finally, we overview some open problems and our future work before concluding the paper.

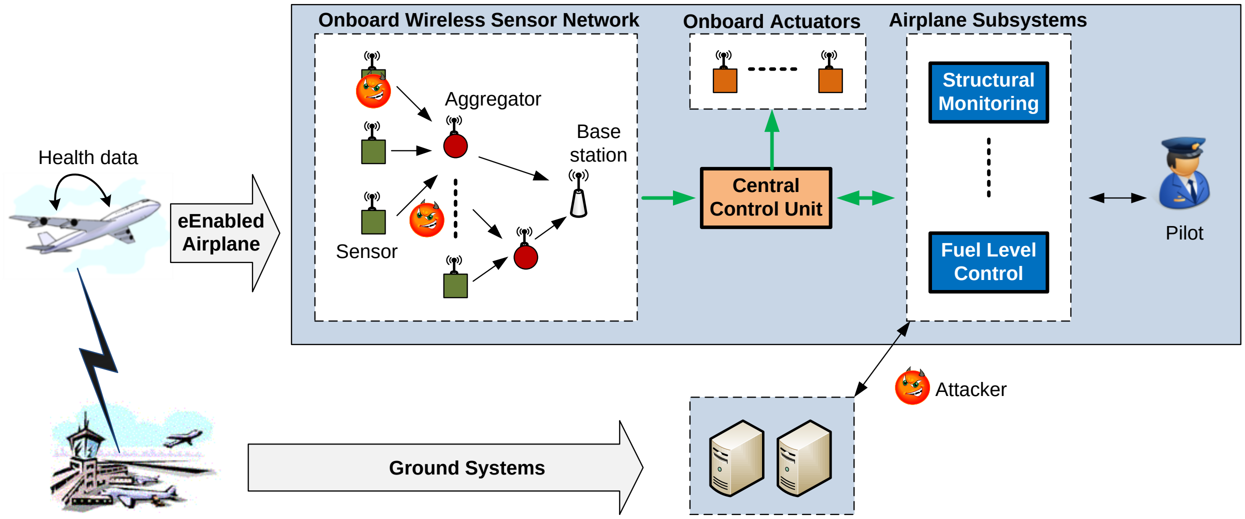

Figure 2. Illustration of the AHMMS model considered. The thick green arrows denote wired and trusted communication links, and the thin arrows denote wireless untrusted communication links.

System Model

Fig. 2 illustrates the generic AHMMS model considered in this paper. The WSN consists of battery-operated smart sensors (nodes) that possess a signal processing unit, memory and a wireless communication unit deployed over the airplane structure and onboard systems for health monitoring. These sensors can be heterogeneous in capabilities (e.g. node transmission range) and modalities (e.g. vibration, temperature, pressure etc). Due to their limited battery power, multi-hop routes are employed in the WSN where each sensor node communicates directly with one-hop neighbors, i.e. nodes in its radio range. Further to reduce the overwhelming volume of data in the AHMMS, we assume in-network data aggregation or data fusion in the WSN [11]. The aggregator nodes forward data to a base station that in turn provides this feedback to a central control unit. The feedback is finally sent to the intended airplane subsystems. The data collection in the WSN can be done periodically, or upon detection of an event by one or more sensors (e.g. abnormal increase in structural temperature) or on demand by an airplane subsystem or a control unit (e.g. query to determine the fuel level).

The airplane subsystems analyze the feedback received from sensors owned and/or operated by them. The analysis can lead to execution of tasks at the subsystems, such as triggering onboard actuators via the central control unit or initiating downlink of detected airplane faulty parts diagnostic data to the ground systems. The authorized ground systems of airplane owners (airlines) also are capable of initiating download of health data when their airplanes are on the ground and/or in flight.

System and Trust Assumptions

The AHMMS is assumed to be administered in such a way that access privileges are assigned and managed appropriately. Passwords and private keys are kept secret, and digital certificates are properly managed and protected. The networks used for health data distribution to ground systems are assumed to be robust against well known denial of service attacks. As a backup mechanism for addressing network systems failure, data distribution via physical media is assumed and is considered adequate to meet requirements for timely data delivery from an aircraft. Further, the airplane owner is trusted to be capable of managing the avionics including the configuration of the AHMMS reliably and correctly.

The wireless sensors are assumed to not degrade despite the harsh flight conditions such as high temperatures and high acceleration vibrations. Further, it is assumed that sufficient physical security checks are in place to prevent unauthorized cabin access to onboard systems and sensors.

While the onboard wired network is trusted and protected from any unauthorized access, the onboard WSN cannot be trusted due to the easy access to wireless sensor communications. For example, the proposed onboard use of personal wireless-enabled electronic devices [17], such as PDAs and cell phones, raises a potential vulnerability for unauthorized onboard access to AHMMS WSN communications.

We assume that onboard sensors for assessing safety-critical parts and systems are subject to physical checks when validating airworthiness of the airplane; additionally these sensors have a backup hard-wired connection to the control unit to enable cross checks for verifying consistency of the generated wireless readings or alarms. Nevertheless, use of wireless networks allows an adversary to perform remote attacks that can manipulate avionics operation in unexpected ways.

Adversary Model

The adversary can be external to the AHMMS and/or an insider. We consider the adversary to be capable of passive attacks (network traffic analysis) as well as active attacks such as node impersonation attack and compromise of sensors (node capture [14]). It is also assumed that the adversary is capable of performing denial of service attacks on the WSN by jamming the wireless channels [12].

We note that insider attacks based on compromised sensors 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 insider threats for rigor and completeness of our security analysis. We present potential IT solutions which can enhance the level of protection to avionics systems.

The overall objective of the adversarial attacks is to either lower safety margins of airplanes or induce unwarranted delays and expenses for airplane owners.

Security Threats

Based on the expected impact of adversarial attacks, we identify the following classes of security threats.

Safety Threats

The adversary may attempt to manipulate health data with the intention of hiding or delaying detection of safety-critical faults in the airplane to potentially induce flight hazards. The manipulation may be done by corrupting, replaying, or blocking the data during its collection and/or distribution. However, since we assume that onboard safety-critical sensing and actuations are also hard-wired to the central control unit, most of the attacks that generate alerts during real-time airplane operation can be successfully thwarted by additional consistency checks at the control unit. Nevertheless, by hiding onboard safety-critical detections during their distribution to ground systems, the adversary may still be able to lower airplane safety margins. Further, the adversary may passively eavesdrop on safety-critical health data to derive information that may be leveraged for other attacks. Although the above two threats do not induce immediate hazards for flights, they may be exploited for future attacks.

Business Threats

In addition to the threats that induce flight hazards, the manipulation of health data can induce delays and costs that impede business of the airplane owner significantly. For instance, the adversary may engineer sufficient false alarms during onboard or off-board diagnosis of the health data feedback, to reduce the reliability and confidence in the AHMMS health assessments. Further, late detection of onboard faults can also induce unwarranted flight safety concerns.

Securing Data Collection by WSN

In order to mitigate the above threats to the health data collection by the WSN, we propose the following security primitives.

Integrity

The WSN must be protected from unauthorized modification of data by an adversary attempting to hide, for example, an abnormal decrease in tire pressure. Hence, data received by a sensor/aggregating node/ control unit must be identical to (or an aggregate of) data sent by the originating sensor.

Authenticity

Further, the WSN must also be protected from injection of misleading data by unauthorized and authorized nodes. In order to prevent the external adversarial attacks, upon receiving data, all WSN nodes must be able to verify the validity of both the source and the message. For defending against compromised nodes, the WSN can employ distributed solutions, such as a majority voting scheme where local nodes can jointly determine the validity of an alarm raised by a neighbor based on their own readings [13].

Confidentiality

Communications in the WSN that contain proprietary data and/or sensitive data capable of aiding future attacks (e.g. engine fuel level) must be protected against passive eavesdropping on the wireless channels.

For providing integrity, authenticity and confidentiality of WSN communications, cryptography solutions can be used. Since the sensors are limited in terms of battery power, symmetric cryptography is preferred in WSNs as opposed to asymmetric cryptography which is relatively computation and communication intensive. At the same time, for higher capable nodes in the WSN such as base station and aggregators, asymmetric cryptography based solutions such as digital signature [8] can be used to communicate with other onboard subsystems. Further, in the AHMMS WSN, solutions based on link layer cryptography, i.e. using a cryptographic key shared by two neighbors, are more suited, when compared to solutions based on end-to-end cryptography, i.e. using a key that is shared by each originating sensor and the end destination which can be an aggregator, a sensor, or the base station). However, the link keys must be established by the WSN nodes upon deployment, warranting the following primitive.

Link Key Establishment

The deployment of sensors in many WSN applications, e.g. remote surveillance and animal habitat monitoring, is random. The unknown topology of the network in such applications complicates the key establishment [14]. However, the topology of the AHMMS WSN is assumed to be pre-determined before deployment, hence simplifying key establishment. A potential solution can be based on the tamper-resistant base station that shares a pre-distributed pairwise key with each sensor node before deployment. In such an approach, two neighboring sensor nodes can later establish their link keys via the base station. On the other hand, administration of keying material in the AHMMS is challenging as will be discussed later.

The use of cryptographic solutions, however, is insufficient to prevent attacks in wireless networks. Wireless jamming and *side channel attacks* by compromised/captured sensors are possible [12] [13]. Therefore, additionally, we propose following primitives for AHMMS WSN.

Mitigation of Channel Jamming

The adversary can, for example, employ jamming attacks to block or delay safety-critical fault detections from propagating towards the base station. Therefore, channel jamming attacks must be detected as soon as possible and mitigated in the WSN. A potential solution is in [12], where a network node adjusts its transmission rate in order to contain jamming interference.

Secure Routing

The sensors in WSN need to route their readings timely and reliably even under attacks. The WSN routing protocol must be robust to jamming attacks that induce long and energy-inefficient routes. The routing protocol must also be robust to attacks based on misleading routing messages. For example, if geographic routing is used then by spoofing location information (e.g. the wormhole attack [13]) a compromised node can modify routes as desired by it.

Secure Location Verification

Sensor readings are only useful when associated with their physical locations. For example, sensor data that represents a detected crack in the aircraft structure will be useless if it does not include a physical location for the crack. Further, network services, such as geographic routing, depend on the node location information. Hence, nodes in the WSN must be capable of securely verifying the location claims made by their neighbors to address attacks based on misleading location data, e.g. the wormhole attack on geographic routing [13]. Secure location verification also provides another level of source authentication using the position of a neighbor to verify validity of data received from it.

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

Robustness to Node Capture

For addressing insider attacks based on compromised sensors, tamper-proof sensor hardware offers one potential solution. However, since this solution is expensive and adds to avionics overhead, the design of WSN algorithms for all the above primitives must be capable of tolerating compromise of a fraction of network nodes [14].

Early and Correct Detection of Manipulation

Any manipulation of the health data during collection in the WSN must be detected as soon as possible, while false alarm detections must be avoided.

Challenges in Avionics Systems

In this section, we discuss the impact of main constraints of the AHMMS on solutions used for securing the onboard WSN.

Power-efficiency

Similar to current avionics systems, it is reasonable to assume that the onboard WSN of the AHMMS will be periodically maintained. The sensors must be able to operate reliably on their battery power within this period which can vary in range of several days to weeks. Hence, to conserve the battery power of the WSN nodes, a combination of sensor processing and energy-efficient data aggregation algorithm is needed. Further, the WSN medium access algorithm employed must also be energy-efficient, such as by making nodes to be in sleep mode when not active [2]. Additionally, the solution design for the above primitives must incorporate this energy constraint. For example, given that for sensors a communication costs more power than a computation, energy-efficient secure broadcast routing algorithms are studied in [15].

Low End-to-End Latency

It is pivotal that all detected safety-critical faults must be timely delivered by the WSN to the central control unit for real-time diagnosis [18], and if needed to the ground systems for further analysis. Consequently, the WSN routing algorithms must be designed to be energy-efficient under a given delay constraint.

Traceability under Data Aggregation

Traceability of authorized actions taken in the avionics systems is inherently important. However, use of data aggregation obscures traceability of data in the WSN, reducing, in most cases, the ability to identify the source of the false or malicious fault detection data. The data aggregation algorithm employed in the WSN must address this tradeoff.

Network Membership Dynamics

As other avionics systems, nodes in the WSN can be expected to be removed or replaced over time. Consequently, the key management scheme and policy must allow additions and deletions of nodes from the WSN, while also ensuring secure periodic key updates in the network.

Securing Data Distribution to Ground

While symmetric cryptography and link keys are more suited for data collection in the WSN, asymmetric cryptography based end-to-end solutions are more secure and practical for health data distribution between airplane and ground systems [16]. Similar to the WSN, integrity, authenticity and confidentiality must be provided when communicating health data from airplane to ground systems.

In [8] and [9], we have proposed the use of digital signatures to provide end-to-end integrity and authenticity and defend against external adversary attacks. Signatures can also support traceability and non-repudiation of actions taken onboard as well as on the ground, hence mitigating insider attacks. For confidentiality, asymmetric or symmetric encryption can be additionally used.

For more details, we refer the reader to [8] and [9], where we have employed the Common Criteria (CC) methodology for developing a complete analysis of the security of data distribution between airplane and ground systems.

Discussion and Open Problems

Security Specification for Airworthiness

All aviation industry partners including manufacturers, airlines, servicers, and regulatory institutions are invested in assuring and maintaining continued airworthiness. To define security requirements for airworthiness in a systematic manner, we have contributed a standardized framework based on the CC methodology to identify requirements for securing the electronic distribution of airplane loadable software and data [9]. The standardized approach is taken to enable the extension of our framework into the existing certification guidelines for commercial airplanes. Additionally, in [16], we have investigated impact of the use of cryptography based solutions on the avionics and ground systems operated by eEnabled airplane owners.

RFID System Integration

Our future work will explore extending the framework presented in this paper, to include onboard data generated by radio frequency identification (RFID) systems. The use of an onboard RFID system can be very beneficial for enhancing flight logistics and maintenance application. Further, RFID is considered as a power-free wireless sensor, since it is a passive radio technology operating from the radio energy emanated from a remote reader. Hence, it has advantageous uses in energy-efficient aircraft structural monitoring as well.

Secure Control of Commercial Airplanes

In this paper, we did not consider the real-time control of a commercial airplane by the onboard as well as ground controller based on the feedback from the WSN. Real-time control of commercial airplanes in the national air space is significantly beneficial for the next-generation air transportation system. However, related challenges remain to be fully addressed, including the instability of network control systems [18] and the security of networked control. Some potential solutions may be found in the area of ground control of unmanned aerial vehicles in military applications.

Conclusions

Based on our ongoing investigation, in this paper we provided an overview of our proposed framework for the secure use of wireless sensor networks (WSNs) in commercial airplane health monitoring and management system (AHMMS). Compared to other WSN applications with random sensor deployments, such as animal habitat monitoring, the pre-determined and fixed deployment of the AHMMS can allow use of simplified solutions such as base station approach to key establishment. However, other constraints such as low end-to-end delay and traceability impose major challenges to the design of secure and energy-efficient solutions for addressing threats due to side channel attacks on the AHMMS WSN. Based on our previous work, we proposed the use of digital signatures for the secure distribution of the WSN collected health data to the ground systems.

While in this paper we have identified the main classes of threats and potential defense mechanisms for the AHMMS, our future work will provide a more rigorous and comprehensive security analysis, and evaluate performance of the recommended solutions.

References

[1] Domingo, R., 2006, Health Monitoring and Management Systems (HMMS), US/Europe International Aviation Safety Conference.

www.faa.gov/news/conferences/2006_us_europe_conference/presentations/media/HMMS.ppt

[2] Bai, H., M. Atiquzzaman, D. Lilja, 2004, Wireless Sensor Network for Aircraft Health Monitoring, Broadband Networks (BROADNETS).

[3] Harman, R. Wireless solutions for aircraft condition based maintenance systems, IEEE Aerospace Conference, 2002, pp. 6-2877-6-2886.

[4] Ramamurthy, H., B. Prabhu, R. Gadh, 2004, Reconfigurable Wireless Interface for Networking Sensors (ReWINS), IFIP International Conference on Personal Wireless Communications (PWC), pp. 215-229.

[5] Wargo, C., C. Dhas, 2003, Security considerations for the e-enabled aircraft, Aerospace Conference, pp. 4_1533-4_1550.

[6] Federal Aviation Administration, 2007, 14 CFR Part 25, Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security—Isolation or Protection from Unauthorized Passenger Domain Systems Access, [Docket No. NM364 Special Conditions No. 25–07–01–SC], Federal Register, Vol. 72, No. 71. http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf

[7] Federal Aviation Administration, 2007, 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. http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf

[8] Robinson, R., M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, 2007, Challenges for IT Infrastructure Supporting Secure Network-Enabled Commercial Airplane Operations, AIAA Infotech@Aerospace Conference.

[9] Robinson, R., M. Li, K. Sampigethaya, R. Poovendran, S. Lintelman, D. von Oheimb, J. Buer, J. Cuellar, 2007, Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety, to appear in International Conference on Computer Safety, Reliability and Security (Safecomp).

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

[11] Ou, J., H. Li, 2003, Wireless sensor information fusion for structural health monitoring, Proceedings of the SPIE, Vol. 5099, pp. 356-362.

[12] Li, M., I. Koutsopoulos, 2007, R. Poovendran, Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks, IEEE INFOCOM, pp. 1307-1315.

[13] Lazos, L., R. Poovendran, 2005, SeRLoc: Robust Localization for Wireless Sensor Networks, ACM Transactions on Sensor Networks, Vol. 1, No. 1, pp. 73-100.

[14] Tague, P., R. Poovendran, 2007, A Canonical Seed Assignment Model for Key Predistribution in Wireless Sensor Networks, to appear in ACM Transactions on Sensor Networks.

[15] Lazos, L., R. Poovendran, 2007, Power Proximity Based Key Management for Secure Multicast in Ad Hoc Networks, ACM Journal on Wireless Networks (WINET), Vol. 13, No. 1, pp. 127-148.

[16] Robinson, R., M. Li, K. Sampigethaya, R. Poovendran, S. Lintelman, D. von Oheimb, J. Buer, 2007, Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes, to appear in AIAA ATIO.

[17] Radio Technical Commission for Aeronautics (RTCA), 2006, Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDs) on Aircraft, RTCA/DO-294B.

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