SECURITY OF WIRELESS SENSOR NETWORK ENABLED HEALTH MONITORING FOR FUTURE AIRPLANES

Krishna Sampigethaya*, , Radha Poovendran* , Mingyan Li** , Linda Bushnell* , Richard Robinson****
***EE Department, University of Washington, Seattle, WA, USA**
****Boeing Phantom Works, Bellevue, WA, USA**

Keywords: *Security, Wireless, Sensor, RFID, Airplane Health Management*

Abstract

Wireless technologies are potential drivers for future e-enabled airplane health management (AHM) which is envisioned to be real-time, continuous and proactive. This paper considers the beneficial and secure use of wireless sensors and radio-frequency identification system in AHM. We identify vulnerabilities in e-enabled AHM that can pose concerns with aircraft maintenance, present requirements and potential solutions to mitigate emerging threats, and discuss major challenges. We also present some important issues with potential use of wireless sensors for real-time aircraft operation and control.

1 Introduction

Advances in information technologies, such as the global positioning system, sensors and wireless networking, have brought the aviation industry to the era of the e-enabled airplane [5]. With its revolutionary systems and applications for data collection, processing and distribution, the e-enabled airplane promises to improve the safety, capacity, efficiency and environmental footprint of air transportation. This paper focuses on systems and applications that can improve e-enabled airplane health management (AHM) [1].

A major goal of AHM is to improve maintenance costs and lifetime of aircraft, such as by impacting aircraft availability, aircraft maintenance scheduling, flight cancellations, flight delays, and flight turnaround times [8]. Sensor systems play a key role in meeting this goal by offering a means for monitoring, diagnosing and predicting health of airplanes. Today, wired sensors are used for monitoring the condition of aircraft engines, structures, gear boxes, and so on [8].

Wireless sensor network (WSN), i.e., smart sensors with radio interfaces, promises unprecedented operational benefits to the AHM. For example, reduced airplane wiring costs because cabling is limited to some scenarios such as when sensor power is scavenged from an external resource, and flexibility to be deployed on legacy airplanes for monitoring aging parts without requiring a redesign of data wiring layout [2, 3, 4]. The use of radio frequency identification (RFID) system with passive-only tags in the next-generation airplanes shows the growing prospects of a onboard WSN. As noted in [10], the RFID system can be considered to be a WSN that "senses" information from tags attached to devices. In the context of airplanes, these tagged devices include the onboard line-replaceable units, passenger baggage, and so on [11, 6].

However, as evident from recent airplane regulations and certification conditions [12, 13, 14], the demands on new onboard wireless technologies can be expected to be heavy. Safety concerns with these technologies are primarily focused on impact of radio interference on the operation of other onboard systems, requiring isolation or prevention measures such as limitations

on their use, e.g., "sensing" by RFID readers is done only when airplanes are on the ground [14]. Security concerns, on the other hand, need a careful assessment of threats and their prevention or mitigation. Therefore, with the potential future use of vulnerable wireless solutions for health data collection and distribution, the emerging security threats must be addressed.

WSN and active RFID system have vulnerabilities that can be exploited to deteriorate the reliability, accuracy and availability of health diagnostics and prognostics, impeding beneficial uses of the AHM (see Section 2.3). This paper addresses such threats to the business of the AHM. Additionally, the paper discusses threats that can arise if e-enabled health data is used in real-time flight-critical operation and control.

The remainder of this paper is organized as follows. Section 2 presents the system model and the types of adversarial attacks considered, followed by the resulting security threats to wireless AHM. Section 3 proposes security requirements for health data collection and Section 4 discusses security of health data distribution. Section 5 discuss challenges that must be addressed for using proposed security solutions as well as for future WSN-enabled flight operation and control. Section 6 presents our conclusions and future work.

2 AHMMS Model Considered

Fig. 1 illustrates the generic model in this paper referred as Airplane Health Management and Monitoring System (AHMMS), including onboard health data collection by a central control unit and health data distribution to ground systems of airlines. As shown, we consider the use of wireless sensors, wireless access points and active RFID system for collecting business-critical health data only, and assume that all safety-critical data collection is by protected wired sensors.

The WSN consists of smart sensors which are battery-powered[1], possessing a signal processing unit, memory, and a wireless data 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-energy, 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 [18]. The aggregator nodes forward data to a local control unit which in turn provides this feedback to a central control unit. The data collection in the WSN can be done periodically, or upon detection of an event by one or more sensors (e.g., abnormal structural temperatures) or on demand by an airplane subsystem or the control units (e.g., fuel level queries). Further, the onboard RFID system consisting of active tags and readers shown in Fig. 1, is used to collect onboard part maintenance information and forward to the central control unit.

Upon receiving feedback from the local control units, the central control unit forwards data to the airplane subsystems owning the sensors. The subsystems perform diagnosis, i.e., locating and describing existing failures, and prognosis, i.e., locating and describing potential failures [9]. The analysis can lead to execution of tasks at the subsystems, such as triggering onboard actuations via the central control unit or initiating a downlink of detected airplane faulty part diagnostics to the ground systems as shown. The authorized ground systems of airlines are also capable of initiating a download of health data when their fleets are on the ground and/or in flight.

2.1 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 sys-

[1] In some cases, it maybe possible to scavenge power from the sensor-residing system instead of a battery.

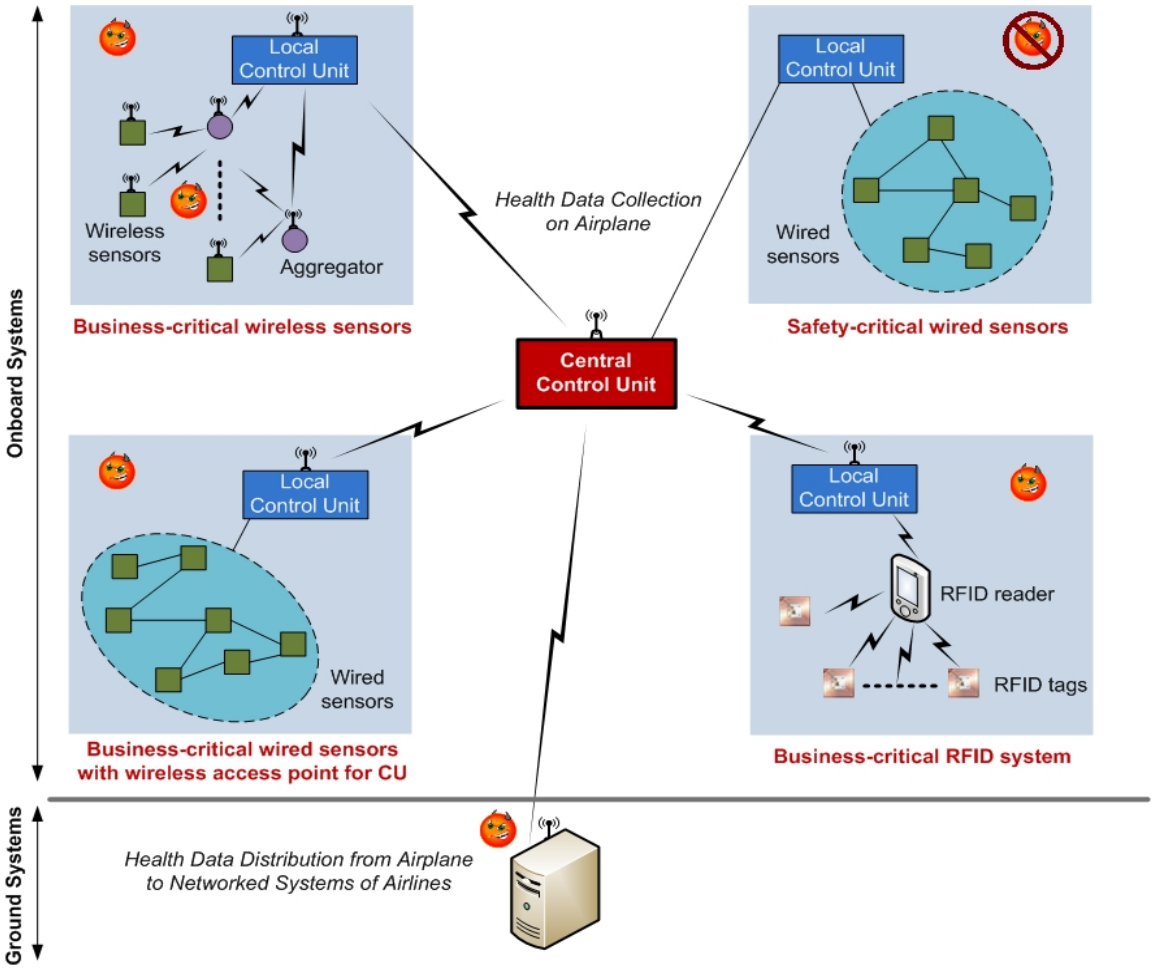

Fig. 1 Airplane Health Management and Monitoring System (AHMMS) Model. Solid lines are wired links.

tems 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, airlines are trusted to be capable of managing the AHMMS configuration reliably and correctly.

The sensors are assumed to be resilient to harsh flight conditions such as high temperatures and acceleration vibrations. Additionally, 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, RFID system and wireless interfaces cannot be trusted due to the easy access to RF communications. For example, the proposed onboard use of transmitting personal electronic devices [25] which can include laptops, RFID tags and cell phones, raises a potential vulnerability for disruption or unauthorized access to health data communications. Therefore, use of wireless networks can allow an adversary to perform remote attacks, manipulating AHMMS operation and availability in unexpected ways.

2.2 Adversary Model

The overall objective of the adversarial attacks considered is to induce unwarranted delays and expenses for owners of the e-enabled airplane. The adversary can be external to the AHMMS and/or an insider. We assume the adversary to be capable of passive attacks (network traffic anal-

ysis) as well as active attacks such as node impersonation attack, compromise of sensors (node capture [22]), tags and readers. It is also assumed that the adversary is capable of performing denial of service attacks on data collection by jamming the wireless channels [19].

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 insider threats for rigor and completeness of our security analysis. We present potential solutions which can enhance the level of protection to airplane systems.

2.3 Security Threats

The adversary may attempt to manipulate health data with the intention of hiding or delaying fault detection in the airplane to potentially induce delays and costs that significantly impede airline business. The manipulation may be done by corrupting, replaying, or blocking the data during its collection and/or distribution in the AHMMS. 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 level of confidence in the AHMMS health assessments. Further, any late detection of onboard faults can induce unwarranted flight safety concerns.

3 Securing Wireless Health Data Collection

In order to mitigate the above threats to the health data collection, we propose the following security primitives for WSN and RFID systems.

3.1 Integrity and Authenticity

Sensor data, e.g., an abnormal decrease in tire pressure, and tag data, e.g., part maintenance information, must be protected from any unauthorized modification by an adversary. Hence, data received by a sensor or aggregating node or reader or control unit must be identical to (or an aggregate of) data sent by the originating sensor or tag. Further, injection of any misleading data into the WSN or the tags by unauthorized and authorized nodes must be prevented.

To prevent attacks by an external adversary, upon receiving data, all sensor nodes must be able to verify the validity of both the source and the message. For the RFID system, it has to be guaranteed that only the authorized readers can write to the tags. Additionally, the readers must be able to authenticate the tags to prevent any corrupted data being scanned from compromised tags, e.g., fake or cloned tags hidden onboard. Hence, mutual authentication is needed between tags and readers. Further, for defending against insider attacks by compromised nodes, potential distributed solution approaches for the WSN and RFID system include majority voting or reputation-based schemes, where local nodes can jointly determine the validity of an alarm raised by a neighbor based on their direct and indirect observations [21].

3.2 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. Similarly, part maintenance history and other data stored in tags must be protected if they have business value or contain proprietary information of the system owner. Although physical security control ensures the first line of defense, encryption is preferred as the wireless links can be intercepted by an adversary without physical access if the transmission power is sufficiently high.

3.3 Efficient Cryptography Schemes

For providing integrity, authenticity and confidentiality of WSN and RFID communications, cryptography solutions can be used. However, since sensors can be limited in terms of battery power, symmetric cryptography is preferred in WSNs as opposed to asymmetric cryptography which is relatively computation and communica-

tion intensive. At the same time, for protecting communications between onboard systems and higher capable nodes in the WSN, i.e., local control units and aggregators, asymmetric cryptography based solutions such as digital signatures can be used.

On the other hand, for the RFID system, only the tags have limited memory, constrained communication range and scarce energy. Therefore, efficient asymmetric key cryptography schemes, such as elliptic curve cryptography, have been shown to be feasible for RFID authentication [20]. Comparatively, symmetric key based authentication with a shared key between a tag and a reader is vulnerable to the compromise of either authenticating entity, and can incur prohibitive overhead from compromise of a reader since all tags that share a pair-wise key with the compromised reader must be securely updated with the new keys.

Further, in the WSN, solutions based on link layer cryptography, i.e., using a cryptographic key shared by two neighbors, are more suited, when compared to solutions based on end-to-end cryptography, i.e., using a key shared by each originating sensor and the end destination which can be an aggregator, sensor, or control unit. However, the link keys must be established by the WSN nodes upon deployment, warranting the following primitive.

3.4 Sensor Pairwise 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 [22]. 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 a tamper-resistant local control unit 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 local control unit. On the other hand, administration of keying material in the AHMMS is challenging as will be discussed later.

Another major threat to both WSN and RFID systems is from wireless jamming attacks [19, 20]. Therefore, we propose the following primitive.

3.5 Mitigation of Jamming

Leveraging the broadcast medium of wireless channels, the adversary can employ jamming attacks to block or delay fault detections from propagating towards the control units. Similarly, the wireless communications between RFID tags and readers are inherently subject to jamming attacks. Therefore, channel jamming attacks must be detected as soon as possible and mitigated in the WSN and RFID system.

The conventional defense strategy against jamming, i.e., spread spectrum, is resource consuming to be deployed in tags and sensors. The detection and defense of jamming attacks launched in different layers of network have been an active research area, and interested readers are referred to [19] for more recent research advance. A potential solution is also in [19], where a network node adjusts its transmission rate in order to contain jamming interference.

3.6 Mitigation of WSN Side Channel Attacks

The use of cryptographic solutions and jamming defense mechanisms, however, are insufficient to prevent side channel attacks by compromised/captured sensors in the WSN [21].

3.6.1 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 [21]) a compromised node can modify routes as desired by it.

3.6.2 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 [21]. 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 time-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.

3.6.3 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 [22].

3.7 Early & Correct Detection of Corruption

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

4 Securing Wireless Health Data Distribution

For health data distribution from airplane to ground, asymmetric cryptography based end-to-end solutions are more secure and practical [24]. Similar to WSN and RFID communications, integrity, authenticity and confidentiality must be provided to protect health data distribution from the adversary.

In [15, 16], 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 [16] 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.

5 Challenges and Open Problems

5.1 Wireless Sensor Capabilities

Sensor communications incur overhead in terms of energy and bandwidth resources which maybe limited in the airplane environment. More processing at smart sensors can reduce this overhead. However, at the same time it can introduce vulnerabilities due to the level of criticality placed on the wireless communication. For example, instead of communicating the redundant raw data a wireless sensor processes the raw data and self-predicts a time-critical fault, the wireless sensor(s) must now communicate this self-prognosis to the central control unit reliable, accurately and timely.

5.2 Power Efficiency of WSN and RFID

Similar to avionics, it is reasonable to assume that the onboard sensors and active tags of the AHMMS will be periodically maintained. The sensors and tags 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 sensor 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 ac-

tive [2]. Additionally, the solution design for the above primitives for WSN and RFID system must incorporate this energy constraint. For example, given that communication costs more power than a computation, energy-efficient secure broadcast routing algorithms for WSN [23] and energy-efficient authentication protocols for RFID [20] are desirable.

5.3 Low End-to-End Latency in WSN

It is pivotal that all detected critical faults must be timely delivered by the WSN to the central control unit for real-time diagnosis [26], 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.

5.4 Traceability in WSN

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.

5.5 WSN and RFID Membership Dynamics

As other avionics, sensors and tags 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 resource-constrained WSN and RFID systems, while also ensuring secure periodic key updates in the network. For the RFID system, the use of asymmetric key cryptography based schemes for mutual authentication will mandate the management of digital certificates. In [20], various approaches with related overhead and scalability are considered, including a certificate whitelist and a hash-chain based approach [20].

5.6 Wireless Flight Operation & Control

With their unprecedented features, WSNs have the potential for providing additional and timely information to support increased automation as well as real-time decision making in future air transportation systems. However, in such a future application, WSN vulnerabilities can threaten to reduce aircraft safety margins, resulting in possible degradation of airworthiness and operational efficiency of the aircraft. In addition to the security threats in Section 2.3, the manipulation of health data can potentially induce flight hazards. For instance, the adversary may corrupt health data during its collection to hide detection of safety-critical faults. However, since we assume that onboard safety-critical sensing and actuation in the AHMMS are hard-wired to the central control unit, most of the attacks that generate such alerts during real-time airplane operation can be successfully thwarted by additional consistency checks at the control units.

However, it is possible that the adversary may attempt to hide onboard safety-critical detections during their distribution to ground systems. Further, the adversary may passively eavesdrop on safety-critical health data to derive information that may be leveraged for other attacks. Although these two threats do not induce immediate hazards for flights, they may be exploited for future attacks. Therefore, a major challenge in extending the use of wireless technologies from business-critical to safety-critical functions is in identifying and mitigating/preventing threats to flight airworthiness.

5.6.1 Security Specification for Airworthiness

In [16] we define security requirements for airworthiness in a systematic manner. Specifically, we contribute a standardized framework based on the CC methodology to identify requirements for securing the distribution of loadable software and health data between airplane and ground systems [16]. The standardized approach is taken to enable the extension of our framework into the existing certification guidelines for commercial airplanes. Additionally, in [24], we have investi-

gated impact of the use of cryptography based solutions on the avionics and ground systems operated by e-enabled airplane owners.

5.6.2 Networked Control of Airplanes

Apart from real-time operation, WSN feedback and wireless networks can also support real-time distributed control of aircraft by onboard as well as ground controllers [7]. However, related challenges must be fully addressed, including the instability of network control systems [26] 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.

5.6.3 High Confidence WSN and RFID

The airplane is a cyber-physical system on which human lives are dependent [27]. Therefore, high confidence is needed in order to ensure that the airplane can exhibit deterministic behavior. The potential use of WSN and RFID warrants that the onboard network and security protocols are verified and validated at an adequate level of assurance. Further, due to the dynamic nature of WSN, it would be desirable to have visualization tools to assess vulnerabilities and trust in the network. Such tools will allow the operator to assign a level of trust to the data received from a specific node or a group of nodes in the network. However, a related challenge is in finding a balance between flight-operator attention and timely decision making, as described next.

5.6.4 Information Visualization

Visualizing information for an overloaded airplane pilot in safety-related applications is an emerging area of study, e.g., visualization of sensor data for aiding pilots when encountering hazardous airflow scenarios [28]. Hence the network visualization tools for trust and vulnerability assessment in critical decision making mentioned above, must be designed carefully. These tools must help in making real-time and reliable decisions, but only require minimal attention from the operator.

6 Conclusions and Future Work

In this paper, we provided an overview of our proposed framework for the assured use of WSN and RFID for data collection and use of wireless networks for data distribution in airplane health management. Compared to other applications with random sensor deployments, such as animal habitat monitoring, the pre-determined and fixed deployment of AHM WSN can allow use of simplified solutions such as centralized 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 WSN. The successful integration of RFID for AHM depends on the integrity and authenticity of environment and workflow information stored at the tags and the feasibility of efficient asymmetric key based mutual authentication schemes. Further, based on our previous work, we proposed the use of digital signatures for the secure distribution of airplane health data to the ground systems.

While we have identified the main classes of threats and potential defense mechanisms for wireless-enabled AHM, our future work will provide an in-depth security assessment and performance analysis of the recommended solutions.

References

[1] Domingo, R., Health management and monitoring systems, *Proceedings of the USA/Europe International Aviation Safety Conference*, 2006.

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

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

[4] Ramamurthy, H., B. Prabhu, R. Gadh, Reconfigurable wireless interface for networking sensors (ReWINS), *Proceedings of IFIP International Conference on Personal Wireless Communications (PWC)*, 2004, pp. 215-229.

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

[6] Thorne, A., Barrett, D., McFarlane, D., Impact of RFID on aircraft turnaround processes, *University of Cambridge Report - Auto-ID Labs 019*, 2007.

[7] Thompson, H., The use of wireless and Internet communications for monitoring and control, *AIAA International Air and Space Symposium and Exposition: The Next 100 Years*, Dayton, Ohio, July 14-17, 2003.

[8] Staszewski, W., Boller, C., Tomlinson, G. R., (Eds.), *Health Monitoring of Aerospace Structures: Smart Sensor Technologies and Signal Processing*, Wiley, March 2004.

[9] Jaw, L, Recent advancements in aircraft engine health management (EHM) technologies and recommendations for the next step, *Proceedings of Turbo Expo 2005: 50th ASME International Gas Turbine & Aeroengine Technical Congress*, Reno-Tahoe, Nevada, June 6-9, 2005.

[10] Waldrop, J., Engels, D.W., Sarma, S.E., Colorwave: a MAC for RFID reader networks, *Proceedings of Wireless Communications and Networking*, pp.1701-1704, March 2003.

[11] Porad, K., RFID in commercial aviation, *Aircraft technology engineering & maintenance*, Vol. 75, pp. 92-99, April/May 2005.

[12] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing model 787Ű8 airplane; systems and data networks security Ůisolation or protection from unauthorized passenger domain systems access, [Docket No. NM364 Special Conditions No. 25Ű07Ű01ŰSC], Federal Register, Vol. 72, No. 71., 2007, http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf

[13] Federal Aviation Administration, 2007, 14 CFR Part 25, Special Conditions: Boeing model 787Ű8 airplane; systems and data networks security Ůprotection of airplane systems and data networks from unauthorized external access, [Docket No. NM365 Special Conditions No. 25Ű07Ű02ŰSC], Federal Register, Vol. 72, No. 72., 2007, http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf

[14] FAA policy for passive-only RFID devices. FAA Regulatory and Guidance Library Online.

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

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

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

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

[19] 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.

[20] Li, M., Fung, C., Sampigethaya, K., Robinson, R., Poovendran, R., Falk, R., Kohlmayer, F., Koepf, A., Public Key Based Authentication for Secure Integration of Sensor Data and RFID, *Proceedings of ACM workshop on Heterogeneous Sensors*, May 2008.

[21] 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.

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

[23] 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.

[24] Robinson, R., Li, M, Sampigethaya, K., Poovendran, R., Lintelman, S., von Oheimb, D., Busser, J., Impact of public key enabled applications on the operation and maintenance of commercial air-

planes, *Proceedings of AIAA ATIO*, 2007.

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

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

[27] 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.

[28] Aragon, C. R. and Hearst, M. A., Improving aviation safety with information visualization: a flight simulation study, *Proceedings of the SIGCHI conference on Human factors in computing systems*, Portland, Oregon, USA, 2005, pp. 441–450.

Copyright Statement