Studies in the Development of Wireless Sensor Network in Avionics Assuring Robust Communication

Thesis submitted by

Adishesha CS

Doctor of Philosophy (Engineering)

Department of Instrumentation & Electronics Engineering
Faculty of Engineering & Technology
Jadavpur University
Kolkata, West Bengal, India.
2025

Jadavpur University

Kolkata, India

Index No.: 65/18/E

1. **Title of the thesis**: Studies in the Development of Wireless Sensor Network in Avionics Assuring Robust Communication

2. **Name, Designation and Institution of the Supervisor(s)**:

   (a) Dr. Kumardeb Banerjee
   Professor,
   Department of Instrumentation and Electronics Engineering,
   Jadavpur University, Kolkata, West Bengal

   (b) Dr. Mridul Sankar Barik
   Assistant Professor,
   Department of Computer Science and Engineering,
   Jadavpur University, Kolkata, West Bengal

3. **List of Publication**:

   [1] Vadgaonkar, P., Janardhan, U., and Sivaramasastry, A., "Wireless Sensing - Future's Password to Digital Avionics System," SAE Technical Paper 2014-01-2132, 2014, https://doi.org/10.4271/2014-01-2132.

   [2] Thupakula, K., Sivaramasastry, A., and Gampa, S., "A Methodology for Collision Prediction and Alert Generation in Airport Environment," SAE Int. J. Aerosp. 9(1):1-7, 2016, https://doi.org/10.4271/2016-01-1976.

   [3] A. Sivaramasastry, S. K. Das, C. Mazumdar, K. Banerjee and M. S. Barik, "Priority queuing model for analysis of network traffic in flight operations of commercial aircraft," 2017 International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 25-30, https://doi: 10.1109/CCUBE.2017.8394172.

   [4] Jha, A., Sahay, G., and Sivaramasastry, A., "Framework and Platform for Next Generation Aircraft Health Management System," SAE Technical Paper 2017-01-2126, 2017, https://doi.org/10.4271/2017-01-2126.

   [5] Adishesha CS, Prasanna Ramamurthy, Sanjay Bajekal, Kumardeb Banerjee, Robust Wireless Sensor Network for Intra-Aircraft Communication Proceedings of the 4th World Engineers Summit 2019, Singapore, 28-29 Aug 2019.

[6] Adishesha CS, Prasanna Ramamurthy, Mridul Sankar Barik, Kumardeb Banerjee, "A CDMA based approach for QoS improvement in Intra-Aircraft Wireless Sensor Networks (IAWSN)" SAE AeroCON 2024, Bangalore, India, June 6-7, 2024

[7] Adishesha CS, Thirunarayana, A., Shreshthi, M., Barik, M. et al., "Wireless Power Transfer in Aircraft Systems," 2024-01-1927, in the Proceedings of the SAE AeroTech Conference & Exhibition, 2024, North Carolina, USA. https://doi.org/10.4271/2024-01-1927.

[8] Adishesha CS, Mridul Sankar Barik, Kumardeb Banerjee, "Design of A Comprehensive Security Framework for Intra-Aircraft Wireless Sensor Network," communicated to IEEE Access, July, 2025.

4. **List of Patents**:

[1] US010827411B2 "Deployment of a wireless aircraft network" Sivaramasastry, Adishesha Chinknyakanhalli; Prasanna, Ramamurthy; Das, Subhra Kanti; Granted on November 03, 2020.

[2] US010666498B2 "Architecture for wireless avionics communication networks" Sivaramasastry, Adishesha Chinknyakanhalli; Das, Subhra Kanti; Prasanna, Ramamurthy; Granted on May 26, 2020.

[3] US010944623B2 "Prognosis and graceful degradation of wireless aircraft networks" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti, Shreshthi, Mahadevanna; Granted on March 9, 2021.

[4] US010848302B2 "Network security framework for wireless aircraft communication" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti, Lynch, Michael A, Thupakula, Kiran; Granted on Nov 24, 2020.

[5] US010455445B2 "Performance optimization for avionic wireless sensor networks" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti; Granted on Oct 22, 2019

[6] US011153922B2 "DIRECTIONAL WIRELESS COMMUNICATIONS ONBOARD AIRCRAFT", Sivaramasastry, Adishesha Chinknyakanhalli, Shreshthi, Mahadevanna, Prasanna, Ramamurthy; Granted on Oct 19, 2021

5. **Co-Authored Book:**

[1] GVV Ravi Kumar, Seema Chopra, Adishesha CS, V Sudhakar & Satish Thokala, "Integrated Aircraft Health Management for Beginners" © 2023 Aeronautical Society of India (AeSI), New Delhi. ISBN NO: 978-81-972778-4-9 Publication Date: 29-09-2024.

6. **List of Presentations in National/International Conferences/Workshops**:

[1] Presented a paper entitled ”Priority queuing model for analysis of network traffic in flight operations of commercial aircraft,” at the 2017 International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017.

[2] Presented a paper entitled ”Robust Wireless Sensor Network for Intra-Aircraft Communication” at the 4th World Engineers Summit 2019, Singapore, 28-29 Aug 2019.

[3] Presented a paper entitled “A CDMA based approach for QoS improvement in Intra-Aircraft Wireless Sensor Networks (IAWSN)” SAE AeroCON 2024, Bangalore, India, June 6-7, 2024.

[4] Presented a paper entitled ”Wireless Power Transfer in Aircraft Systems,” in the SAE AeroTech Conference & Exhibition, 2024, North Carolina, USA.

PROFORMA - 1

STATEMENT OF ORIGINALITY

I, **Adisesha CS** registered on **01/11/2018** do hereby declare that this thesis entitled "**Studies in the Development of Wireless Sensor Network in Avionics Assuring Robust Communication**" contains literature survey and original research work done by the undersigned candidate as part of Doctoral studies.

All information in this thesis have been obtained and presented in accordance with existing academic rules and ethical conduct. I declare that, as required by these rules and conduct, I have fully cited and referred all materials and results that are not original to this work.

I also declare that I have checked this thesis as per the "Policy on Anti Plagiarism, Jadavpur University, 2019", and the level of similarity as checked by iThenticate software is 7%.

_____

Signature of Candidate:

Date:

_____

Certified by Supervisor 1:

Date:

_____

Certified by Supervisor 2:

Date:

PROFORMA - 2

CERTIFICATE FROM THE SUPERVISOR

This is to certify that the thesis entitled "**Studies in the Development of Wireless Sensor Network in Avionics Assuring Robust Communication**" submitted by **Adisesha CS**, who got his name registered on **01/11/2018** for the award of Ph.D. (Engg.) degree of Jadavpur University, is absolutely based upon his own work under the supervision of **Dr. Kumardeb Banerjee**, Professor, Department of Instrumentation and Electronics Engineering, Jadavpur University, Kolkata, West Bengal and **Dr. Mridul Sankar Barik**, Assistant Professor, Department of Computer Science and Engineering, Jadavpur University, Kolkata, West Bengal, and that neither his thesis nor any part of the thesis has been submitted for any degree/diploma or any other academic award anywhere before.

_____

Signature of the Supervisor 1:

Date:

Dr. Kumardeb Banerjee
Professor,
Department of Instrumentation and Electronics Engineering,
Jadavpur University, Kolkata, West Bengal

_____

Signature of the Supervisor 2:

Date:

Dr. Mridul Sankar Barik
Assistant Professor,
Department of Computer Science and Engineering,
Jadavpur University, Kolkata, West Bengal

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude and regards to my supervisors **Dr. Kumardeb Banerjee,** Professor, Department of Instrumentation and Electronics Engineering, Jadavpur University, Kolkata, West Bengal and **Dr. Mridul Sankar Barik,** Assistant Professor, Department of Computer Science and Engineering, Jadavpur University, Kolkata, West Bengal for their exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The guidance, help and motivation provided by him from time to time is incredible and help me my professional and personal journey in my future days.

I also take this opportunity to express my gratefulness to **Prof. Chandan Mazumdar**, Professor, Department of Computer Science and Engineering, Jadavpur University, Kolkata, West Bengal. He has been a constant source of inspiration as a philosopher and guide to pursue this research work.

I also take this opportunity to express a deep sense of gratitude to the department of Instrumentation & Electronics Engineering, Our respected and honorable head of the department of Instrumentation & Electronics Engineering, **Dr. Prolay Sharma**, for his cordial support, valuable information and guidance, which helped me in completing this task through various stages.

I am greatly thankful to **Collins Aerospace**, my colleagues and the management for providing all necessary support to me in carrying out this research work.

I am obliged to staff members of **Jadavpur University** for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Adishesha CS

This thesis is dedicated to

My Parents

Sri CR Sivarama Sastry and Smt Padma

Contents

List of Figures

List of Tables

Abstract

In this thesis, we have presented research work focused on the development of a wireless sensor network in avionics to ensure robust communication. We have presented a detailed report on the current state of WSN for intra-aircraft communication, opportunities, and challenges in meeting the performance requirements of complex safety critical applications in the operational life cycle of aviation. We have provided analysis of technologies reported in the literature on stringent performance requirements such as selection of robust network architecture, network protocols, and security algorithms to meet the quality of service parameters. We have presented a two-layered architecture for IAWSN, a pre-emptive queueing model for throughput enhancement for variable data type and variable data rates, and a CDMA based approach to mitigate the throughput challenges due to coexistence of multiple networks like Wi-Fi, Bluetooth in presence of various sources of emission and absorption. We have analysed the threat scenarios and presented a comprehensive security framework for IAWSN with lightweight cryptography algorithms, key generation and key management techniques to ensure optimised throughput and robust security in the given use case scenarios. We have discussed the implementation of all the above research outcomes / solutions in the aircraft environment, performance analysis both on simulation platforms and in the lab environment. We have discussed the revision of security algorithms to meet performance requirements. Performance analysis has confirmed that the results of the simulation and experimental studies are satisfactory. Finally, we have presented the use cases of Aircraft Health Management as an application of the proposed WSN that can be scaled up to WAIC band based on AVSI recommendations and ITU approvals. We have further presented a feasibility analysis of the potential use of the proposed IAWSN architecture for Wireless Power Transfer inside aircraft. We have discussed the future scope of this research on network architecture and protocols, detailed threat evaluation, and enhancement of security algorithms to scale up to the 4.2 GHz WAIC band.

List of Abbreviations

AES	Advanced Encryption Standard
AFDX	Avionics Full-Duplex Switched Ethernet
AHM	Airplane/Aircraft Health Monitoring
AHMC	Aircraft Health Management Computer
AI	Artificial Intelligence
API	Application Programming Interface
APT	Acoustic Power Transfer
APU	Auxiliary Power Unit
ARINC	Aeronautical Radio Incorporated
AVSI	Aerospace Vehicle Systems Institute
BER	Bit Error Rate
CAN	Controller Area Network
CBM	Condition Based Monitoring
CDMA	Code Division Multiple Access
CE-LPCP	Collective Encoded Low-Density Parity-Check
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access
CSMA-CA	Carrier Sense Multiple Access - Collision Avoidance
DM	Data Manager
DoS	Denial of Service
DSKC	Dynamic Symmetric Key Cryptography
DSSS	Direct Sequence Spread Spectrum
ECC	Elliptic Curve Cryptography
EED	End-To-End Delay

EEPROM	Electrically Erasable Programmable Read Only Memory
EHM	Engine Health Management
EKE	Encryption Key Engine
EMC	Electromagnetic compatibility
EMI	Electromagnetic Interference
EPS	Electrical Power System
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FDMA	Frequency Division Multiple Access
HILPB	High Intensity Laser Power Beam
IAHM	Integrated Aircraft Health Monitoring
IAWSN	Intra-Aircraft Wireless Sensor Network
IMA	Integrated Modular Avionics
ISM	Industry Science and Medical
ITU	International Telecommunication Union
IVHM	Integrated Vehicle Health Management
IVS	Initialization Vector Sequence
KIDC	Key Index Distribution Center
LED	Light Emitting Diode
LPCP	Low-Density Parity-Check
LPT	Laser Power Transfer
LTE	Long Term Evolution
MAC	Medium Access Control
MAV	Multi- Aerial Vehicle
MEA	More Electric Aircraft
ML	Machine Learning
MRO	Maintenance, Repair and Overhaul
NM	Network Manager
NVRAM	Non Volatile Random Access Memory
OSA	Open System Architecture
OEM	Original Equipment Manufacturers
O-QPSK	Offseet-Quadrature Phase-Shift Keying

PDI	Programmable Data Interface
PDR	Packet Delivery Ratio
PER	Packet Error Ratio
PHM	Prognostics and Health Management
PHY	Physical layer
PRN	Pseudo-Random Number
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RSA	Rivest, Shamir and Adleman
RSSI	Residual Signal Strength Indicator
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automobile Engineers
SGC	Secure Group Communication
SHM	Structural Health Monitoring
SNR	Signal-to-Noise Ratio
SPA	Spacecraft Plug & Play Architecture
TDMA	Time Division Multiple Access
WAIC	Wireless Avionics Intra-Communication
WPAN	Wireless Personal Area Network
WPT	Wireless Power Transfer
WSC	Wireless Sensor Cluster
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Preamble

The aerospace industry is advancing toward the design of more intelligent, connected, and safer aircraft that are reliable, affordable, and accessible to customers across all segments worldwide. Hybrid electric and all-electric aircraft are being developed as relevant technologies mature in the areas of advanced materials, electric power systems, artificial intelligence (AI), machine learning (ML), and autonomy. Aviation research is evolving technologies for demonstrating single-pilot operations, pilot assistance systems, and pilot monitoring systems while exploring the possibility of fully autonomous aircraft. To enhance the safety of passengers, crew, and operators, it is crucial to monitor various health parameters of aircraft. Continuous monitoring of the health status of aircraft flight systems at all levels and during all phases of flight is vital. As part of this effort, health management applications like Prognostics and Health Management (PHM), Engine Health Management (EHM), Structural Health Monitoring (SHM), Aircraft Health Management (AHM), and Integrated Aircraft Health Management (IAHM) are being developed. This necessitates an increased number of sensors and more communication networks inside aircraft. Currently, the primary mode of communication in aircraft relies on wired networks, which complicates the deployment and management of an expanded sensor network. Challenges include selecting and optimally placing sensors and establishing seamless communication between various subsystems.

To monitor the health status of aircraft systems, subsystems, or components effectively and determine any necessary corrective actions, the following sequence of steps must be followed: sensing, acquiring, storing, processing, computing, inferring, and communicating. Key requirements driving these technologies include the availability of data and its effective extraction, storage, processing, presentation, and communication to all stakeholders, while maintaining a sensor network that is available, reliable, scalable, secure, affordable, and robust.

A large number of sensors are deployed to monitor the performance and health status of avionics, engines, cabin environments, and structural components. Modern aircraft, such as Boeing's models, have over 10,000 sensors, while Airbus models feature around 25,000, all connected via wired networks. These systems contain over 100,000 wires, spanning over 400 kilometers and weighing over 5,000 kilograms [1] . Additionally, around 30% of these wires are used to segregate, bundle, and support the wired harnesses to the aircraft structure. Studies suggest that at least 30% of these wires could be replaced with wireless networks [2]. However, the reliance on wired networks adds weight to the aircraft and presents significant challenges related to scalability, configurability, and maintainability due to their fixed nature. Wireless Sensor Network (WSN) technology for internal aircraft applications is rapidly evolving and shows promise in overcoming the difficulties associated with wired networks. WSNs reduce the need for wire harnesses inside the aircraft, thus mitigating the complexities related to the sensor network's enhancement, maintenance, and configuration. Consequently, this shift reduces overall weight and, in turn, helps decrease fuel costs.

Various approaches to architecture, configurations, challenges, and opportunities for deploying Wireless Sensor Networks (WSNs) have been analysed [1] [2]. While wireless technology is increasingly implemented in industrial applications, more work is needed before it can be widely adopted for intra-aircraft applications. Key issues such as signal attenuation, dispersion, and jamming caused by electromagnetic interference (EMI) and electromagnetic compatibility (EMC) effects must be addressed [3]. Additionally, variations in data rate and data type within aircraft can lead to performance degradation in commonly used wireless protocols [4]. Challenges to network performance include selecting a robust network architecture and placing network elements onboard the aircraft to ensure adequate network throughput and data security. Given that avionics communication is safety-critical, it is crucial to understand the network security aspects related to overall aircraft operations. Recent research efforts focus on designing and implementing robust and optimized network security solutions to address various threat profiles in the intra-aircraft environment [5]. In this thesis, we have analysed the technological advancements to date, evaluated the gaps, and developed and tested a hierarchical, fault-tolerant, and scalable architecture for IAWSN, along with communication protocols and a security framework for optimized network performance.

1.2 Motivation

Current Scenario: In modern aircraft, only a limited number of sensors are installed to meet the essential requirements for safe flight. These sensors and avionics systems are connected using wired communication. Most data is utilized in real-time for flight controls and management systems to ensure safety during flight. While critical parameters are recorded by onboard systems, such as flight recorders, there is currently no method

for generating, acquiring, or storing health parameters for all subsystems and components of the aircraft for post-flight analysis and investigation at the MRO centers. The wired harness in aircraft is fixed by design, which restricts the addition of more sensors or components due to the safety-critical nature of these applications, which are governed by certification processes.

Developing new Intra Aircraft Wireless Sensor Networks (IAWSN) presents several design challenges, including the selection of topology, frequency allocation for wireless nodes, and the need to meet performance metrics such as network throughput, system latency, and data quality/integrity. It is essential to consider environmental factors within the aircraft, including sources of electromagnetic radiation emission and absorption, which can lead to signal attenuation, jamming, multipath reflection, and increased susceptibility to threats [2]. Unlike industrial and automotive environments, where infrastructure elements, process components, and signal behaviors are largely predictable, the aircraft environment can be highly dynamic. This variability depends on flight phases, the internal configuration of the aircraft, and the occupancy status and activities of passengers, crew, and cargo [5]. Given the critical nature of missions in aviation, the performance indices for IAWSNs are particularly stringent and require thorough analysis to yield a feasible design.

Need for New Solution(s): Implementing health management schemes necessitates installing tens of thousands of sensors onboard aircraft. However, with the current system, introducing additional sensors is quite challenging. Therefore, there is a need for a reliable, available, scalable, secure, affordable, and robust wireless sensor network to connect these sensors with the avionics systems inside the aircraft [2]. In the pursuit of more electric, intelligent, connected, and safer aircraft, the applications such as Prognostics Health Management (PHM) are essential, and Wireless Avionics Intra Communication (WAIC) will serve as the backbone of this effort.

Way Forward: Significant research has been conducted on aircraft and ground operations sensor networking over the decades. The Aerospace Vehicle Systems Institute (AVSI) has proposed wireless communication systems inside aircraft, and the International Telecommunication Union (ITU) has allocated the WAIC Band, a 200 MHz spectrum (ranging from 4.2 GHz to 4.4 GHz), for exclusive use in intra-aircraft communication [6]. The Federal Aviation Administration (FAA) is currently developing standards for the WAIC band network in collaboration with RTCA.

The aviation industry has recognized the advantages of using the WAIC band over traditional mobile network bands within aircraft [7] [8] [9]. However, research is ongoing to address the challenges associated with implementing the WAIC network. The aircraft cabin and cockpit environments are filled with sources of interference, including EMI and EMC

issues, which can lead to signal attenuation and losses. Key challenges include selecting a robust network architecture, optimizing the placement of network elements onboard the aircraft, and ensuring adequate network throughput and data security. Since avionics communication is critical for the safe operation of the aircraft, both for passengers and crew, it is essential to understand network security, vulnerabilities, and potential threats thoroughly. Consequently, the design and development of robust network security solutions are imperative.

1.3 Scope

The scope of work of this thesis includes the following:

1. An analysis of existing technologies for Wireless Sensor Networks (WSN) and the development of a robust WSN architecture for use in aircraft applications.
2. Evaluation of various WSN technologies and architectures to assess their feasibility and establish a robust IAWSN.
3. An analysis of network throughput for various IAWSN applications.
4. An evaluation of threat landscape and design of a security framework for AIWSN.
5. An analysis of IAWSN performance considering the co-existence of different types of networks to ensure optimal Quality of Service (QoS).
6. An evaluation of the IAWSN framework to demonstrate health management applications and wireless power transfer(WPT).

1.4 Major Contribution of Thesis

The major contributions of this thesis are summarized as follows:

1. **A WSN Architecture for Inside Aircraft Application:** We introduce a layered hierarchical network architecture where sensor clusters communicate wirelessly with data managers while the data managers connect to network managers via wired links [10]. Additionally, we highlight the system's fault tolerance features, which are achieved through spatial and spectral redundancy, operating on the IEEE 802.15.4 protocol in the ISM band.
2. **A Technique for Optimization of WSN Throughput:** We introduce a priority queueing model that incorporates both pre-emptive and non-pre-emptive policies to analyze various Quality of Service (QoS) parameters for assessing network performance. Our simulation results demon-

strate that priority queueing in Intra Aircraft Wireless Sensor Networks (IAWSN) leads to optimized throughput [11].

3. **A Technique for Addressing Co-existence of Networks Inside Aircraft:** We evaluate the feasibility of implementing a CDMA-based communication scheme for IEEE 802.15.4-IAWSN to address throughput issues in IAWSN caused by the coexistence of other wireless devices and network elements utilizing Wi-Fi and Bluetooth technologies [12].

4. **A Security Framework for IAWSN:** We assess the potential threat scenarios and vulnerabilities within Intra Aircraft Wireless Sensor Networks (IAWSN). Our work introduces a robust and optimized security framework incorporating dynamic symmetric key cryptography algorithms and group-based key management techniques. Additionally, we evaluate the network's resilience against various attacks targeting IAWSN [13]. The results of our experiments conducted in a laboratory-scale setup are also presented.

5. **A Framework for Next Generation AHM:** We provide a qualitative analysis of current health monitoring systems and propose an integrated architecture that includes data acquisition, data processing, and data fusion. This architecture is designed to perform diagnostics, prognostics, and decision-making both onboard and off the aircraft. Additionally, we present a methodology for conducting onboard diagnostics and generating in-flight warnings for the crew [14].

6. **A Technique for Wireless Power Transfer using IAWSN Architecture:** We present a trade study on alternative sources of wireless power transfer (WPT) and a feasibility analysis of adopting an Intra Aircraft Wireless Sensor Network (IAWSN) architecture for laser power transfer (LPT) to supply power to feed the remotely placed avionics components [15].

The above research contributions have led to the following list publications, patents and co-authored books:

1. **Publications**:

   [I] Vadgaonkar, P., Janardhan, U., and Sivaramasastry, A., "Wireless Sensing - Future's Password to Digital Avionics System," SAE Technical Paper 2014-01-2132, 2014, https://doi.org/10.4271/2014-01-2132.

   [II] Thupakula, K., Sivaramasastry, A., and Gampa, S., "A Methodology for Collision Prediction and Alert Generation in Airport Environment," SAE Int. J. Aerosp. 9(1):1-7, 2016, https://doi.org/10.4271/2016-01-1976.

   [III] A. Sivaramasastry, S. K. Das, C. Mazumdar, K. Banerjee and M. S. Barik, "Priority queuing model for analysis of network traffic in flight operations of commercial aircraft," 2017 International Conference on

Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 25-30, https://doi: 10.1109/CCUBE.2017.8394172.

[IV] Jha, A., Sahay, G., and Sivaramasastry, A., "Framework and Platform for Next Generation Aircraft Health Management System," SAE Technical Paper 2017-01-2126, 2017, https://doi.org/10.4271/2017-01-2126.

[V] Adishesha CS, Prasanna Ramamurthy, Sanjay Bajekal, Kumardeb Banerjee, Robust Wireless Sensor Network for Intra-Aircraft Communication Proceedings of the 4th World Engineers Summit 2019, Singapore, 28-29 Aug 2019.

[VI] Adishesha CS, Prasanna Ramamurthy, Mridul Sankar Barik, Kumardeb Banerjee, "A CDMA based approach for QoS improvement in Intra-Aircraft Wireless Sensor Networks (IAWSN)" SAE AeroCON 2024, Bangalore, India, June 6-7, 2024

[VII] Adishesha CS, Thirunarayana, A., Shreshthi, M., Barik, M. et al., "Wireless Power Transfer in Aircraft Systems," 2024-01-1927, in the Proceedings of the SAE AeroTech Conference & Exhibition, 2024, North Carolina, USA. https://doi.org/10.4271/2024-01-1927.

[VIII] Adishesha CS, Mridul Sankar Barik, Kumardeb Banerjee, "Design of A Comprehensive Security Framework for Intra-Aircraft Wireless Sensor Network," communicated to IEEE Access, July, 2025.

2. **Patents**:

[I] US010827411B2 "Deployment of a wireless aircraft network" Sivaramasastry, Adishesha Chinknyakanhalli; Prasanna, Ramamurthy; Das, Subhra Kanti; Granted on November 03, 2020.

[II] US010666498B2 "Architecture for wireless avionics communication networks" Sivaramasastry, Adishesha Chinknyakanhalli; Das, Subhra Kanti; Prasanna, Ramamurthy; Granted on May 26, 2020.

[III] US010944623B2 "Prognosis and graceful degradation of wireless aircraft networks" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti, Shreshthi, Mahadevanna; Granted on March 9, 2021.

[IV] US010848302B2 "Network security framework for wireless aircraft communication" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti, Lynch, Michael A, Thupakula, Kiran; Granted on Nov 24, 2020.

[V] US010455445B2 "Performance optimization for avionic wireless sensor networks" Sivaramasastry, Adishesha Chinknyakanhalli, Das, Subhra Kanti; Granted on Oct 22, 2019

[VI] US011153922B2 "DIRECTIONAL WIRELESS COMMUNICATIONS ONBOARD AIRCRAFT", Sivaramasastry, Adishesha Chinknyakanhalli, Shreshthi, Mahadevanna, Prasanna, Ramamurthy; Granted on Oct 19, 2021

3. **Co-Authored Books:**

   [I] GVV Ravi Kumar, Seema Chopra, Adishesha CS, V Sudhakar & Satish Thokala, "Integrated Aircraft Health Management for Beginners" © 2023 Aeronautical Society of India (AeSI), New Delhi. ISBN NO: 978-81-972778-4-9 Publication Date: 29-09-2024.

1.5 Structure of Thesis

Rest of the thesis is organized into following chapters:

Chapter 2: In this chapter, we have reviewed the current research on Intra Aircraft Wireless Sensor Networks (IAWSN). Our comprehensive survey of existing literature has addressed various aspects of avionics sensor networks, including their advantages, limitations, and applications in aviation. We have explored the complexity and critical nature of these networks and relevant guidelines provided by regulations and certifications. Additionally, we evaluated the technological maturity required to deploy robust sensor networks that can effectively scale to meet the demands of health management and wireless power transfer applications. Through our analysis, we identified gaps in the current research landscape and highlighted opportunities for the future to address these gaps. We have formulated a clear problem statement to guide the technical solutions necessary for the successful implementation of IAWSN, which can later be scaled up to Wireless Avionics Intra-Communications (WAIC).

Content of this chapter is based on publications [I, II, IV].

Chapter 3: In this chapter, we have presented an architecture for wireless sensor networks (WSN) specifically designed for communication within aircraft. We have discussed the findings from a comparative study of different networking technologies and architectural concepts, leading to an approach for creating a WSN that is robust, secure, adaptable, and scalable. Additionally, we have addressed the design challenges associated with this architecture. The methodology for integrating various sensor-based applications with a robust network framework is also examined.

Content of this chapter is based on publication [III], patents [III, V] and co-authored book [I].

Chapter 4: In this chapter, we have analyzed the throughput of the proposed Wireless Sensor Network (WSN) across various flight phases. We have developed a priority queuing model that takes into account the varying priorities of sensor data during different stages of flight operations. This model is implemented based on network requirements, and we have examined the traffic distributions relative to the frequency of data transmitted by various sensors at these different phases. Both preemptive and non-preemptive policies are employed to create a stochastic analysis model that assesses different Quality

of Service (QoS) parameters, allowing us to evaluate the network's response to dynamic traffic characteristics.

Content of this chapter is based on publications [III, VI] and patents [III, V].

Chapter 5: In this chapter, we have evaluated the feasibility of deploying Code Division Multiple Access (CDMA) for IEEE 802.15.4-based Intra Aircraft Wireless Sensor Networks (IAWSN) onboard aircraft. This aims to address issues arising from the coexistence of Wi-Fi and Bluetooth as communication mediums and the interference caused by radiating equipment. We have analyzed key Quality of Service (QoS) parameters, including signal-to-noise ratio (SNR), operational bandwidth, bit error rate (BER), and process gain, both with and without CDMA, through simulations. Additionally, we have examined the performance of spread spectrum technology and its impact on the throughput of IAWSN [12].

Content of this chapter is based on publications [III, VI].

Chapter 6: In this chapter, we have presented a security framework for wireless sensor networks (WSN) in aircraft. We propose a hybrid network architecture for communication within the aircraft, followed by optimized security algorithms for key generation and management. These algorithms include Dynamic Symmetric Key Cryptography and Group-Based Key Distribution, along with features for ensuring resilience and fault tolerance. Additionally, we have provided a detailed performance evaluation that assesses the strength of the encryption keys and analyzes both computation and network overhead.

Content of this chapter is based on publication [VIII] and patent [IV].

Chapter 7: In this chapter, we present two applications of the proposed architecture for the Intra Aircraft Wireless Sensor Network (IAWSN) and the Wireless Avionics Intra-Communications (WAIC). (1) Integrated Aircraft Health Monitoring (IAHM): We have conducted a qualitative analysis of existing health monitoring systems and proposed an integrated modular architecture. Additionally, we have provided a framework and platform designed to implement IAWSN for clustered communication among avionics elements. This implementation aims to facilitate computationally intensive prognostics and diagnostic applications, supporting decision-making for Condition-Based Maintenance (CBM). (2) Wireless Power Transfer (WPT): We have explored the potential for deploying Wireless Power Transfer alongside the WAIC strategy. We have presented a comparative study of various wireless power transfer techniques suitable for DC voltage configurations, along with the challenges of meeting certification standards outlined in RTCA DO-160 for EMI, EMC, and power quality in aircraft environments. Furthermore, we have shared analysis and simulation results for different WPT technologies and architectures tailored for aerospace applications.

Content of this chapter is based on publications [II, IV, VII], patent [IV], and co-authored book [I].

Chapter 8: In this chapter, we have provided a comprehensive summary of the thesis and concluded our research work. We aim to clearly identify the opportunities for further investigation, highlighting both short-term and long-term prospects. Given the complexity of the technology and its critical importance for safety in aviation, there is a significant opportunity for collaboration among researchers from various fields for the advancement of aircraft technologies.

Chapter 2

Related Work

2.1 Introduction

In order to realize robust and scalable wireless communications for aircrafts, suitable techniques and protocols need to be formulated. These protocols need to address the challenges in terms of bandwidth allocation for devices, transmission power as well as interference.

2.1.1 Interface Techniques of Wired Sensor Network

At present avionics bus is using Local area networks on most platforms, based on standards specific to aerospace industry, like ARINC 429, AFDX (ARINC 664), MIL-STD 1553, CAN, etc [16]. Wired network poses challenges of scalability, adaptability, increased time and cost to meet the regulatory and certification requirements, due to the fixed nature of architecture.

2.1.2 Future Needs of Sensor Networking

Having a robust network architecture for sensor networking inside aircraft is essential to support scalability and configurability while ensuring reliable communication. The paper by Chen et. al. [17] proposes a method for IP-based communication between aircraft and ground systems, incorporating GPRS and GIS data to predict de-icing requirements. This approach aims to reduce the time aircraft spend on the ground, thus improving operational efficiency. Fitzhugh et. al [18] provide an extensive analysis of electromagnetic interference characterization at the 2.4 GHz ISM band in an aircraft environment. The study highlights the benefits of spatial and spectral diversity in mitigating multipath fading effects within the aircraft. Research [19] investigate the feasibility of using a dedicated frequency band for Wireless Aircraft Intra-Communication (WAIC). It includes experimental results characterizing interference patterns inside the aircraft and cabin systems, particularly in the presence of dynamic

occupancy for the specified frequency spectrum. by Alena et. al. [20] present a trade study that defines an extension to the Spacecraft Plug and Play Architecture (SPA) standards for wireless ZigBee networks, outlining the functions of the SPA-Z Subnet Manager software. The paper [21] discusses the applicability of the IEEE 1451 reference architecture for wireless spacecraft avionics using commercial off-the-shelf (COTS) components. [22] addresses the communication requirements for aerial MAV networks, focusing on technology readiness for inter-MAV communication and identifying areas for future research regarding the feasibility of implementing proposed schemes, as well as reliability and time-critical aspects for large networks. Arms et. al [23] conducted significant research into energy harvesting and network synchronization for structural health management in aircraft to minimize power consumption from aircraft or batteries for sensor network applications. The paper [24] provides a qualitative evaluation of various wireless network technologies, including avionics, wireless network components, security, optical networks, and aircraft safety. [25] details the design and development of wireless sensors for corrosion monitoring in aircraft, proposing the use of COTS components, although it does not address the architecture for a wireless sensor network. [3] presents a comparative analysis of wireless network protocols for industrial wireless communication within wireless aircraft intra-communication networks. The study emphasizes the critical role of MAC protocol performance in ensuring network robustness. Overall, these discussions offer an overview of the maturity of wireless network components for various applications such as aircraft, spacecraft, MAV, and industrial environments. They also present performance analyses of network elements in interfering environments across different frequencies. However, the design elements for a holistic wireless sensor networking architecture inside aircraft remain unaddressed.

To enable wireless communications for aircraft, it is essential to develop suitable protocols that address several challenges, including bandwidth allocation for devices, transmission power, and interference management. Existing literature [2] [26] provides an initial overview of the design specifications and challenges involved in creating protocols for Wireless Sensor Networks (WSN). When designing the wireless network, considerations must include the number of connected nodes, the presence of high and low data rate transmitters, and the need for guaranteed end-to-end delays based on the relative locations of devices. These factors contribute to the specifications for the design of access control protocols. Traffic analysis, through network modeling and simulation, can effectively evaluate the design specifications for wireless network architecture and Quality of Service (QoS) parameters, such as turnaround time, network throughput, system response, and predictability. Additionally, traffic analysis can help estimate power consumption at the sensor nodes by establishing upper bounds for data transmissions. Large-scale WSN models have been analyzed using queueing models [27] [28], and analytical models of Medium Access Control (MAC) protocols have been developed for performance evaluation [29] [30] [31]. Research has also been conducted on the energy requirements and mobility aspects of WSN [32] [33]. However, the current body of knowledge does not

yet encompass parameters specific to avionics and aircraft applications, such as sensor prioritization.

2.2 Sensor Networking Topology

Applications such as Engine Health Monitoring (EHM), Structural Health Monitoring (SHM), Aircraft Health Monitoring (AHM), and Integrated Vehicle Health Management (IVHM) are utilized to monitor the health of aircraft and critical subsystems. Various sensors collect health and usage data, which are then communicated for further processing, monitoring, and control [2] [26]. As modern aircraft become increasingly intelligent, there is a growing demand for a higher number of sensors to enhance health monitoring and automation. This shift leads to heightened requirements for accuracy, safety, and reliability in aircraft functionalities. Currently, sensors are distributed throughout the aircraft and interconnected via a wired network, linking them to processing, monitoring, and control Line Replaceable Units (LRUs) for data communication and signal processing [23]. However, using a wired network poses challenges in terms of cable routing, stray capacitance, mechanical structure, and additional weight. Increased weight negatively impacts fuel efficiency. Additionally, wired networks have limitations regarding flexibility, scalability, configurability, high maintenance costs, and prolonged downtime. This situation creates an urgent need for avionics communication to transition from wired to wireless solutions. Nonetheless, developing new Wireless Sensor Networks (WSNs) comes with its own set of design challenges, such as selecting appropriate topologies, allocating frequencies for wireless nodes, and ensuring Quality of Service (QoS) in terms of network throughput, system latency, and reliable data delivery. It is essential to consider environmental factors within the aircraft, such as sources of electromagnetic radiation that can lead to signal attenuation, jamming, multipath reflection, and increased vulnerability to threats. Unlike the predictable infrastructure and signal behavior found in industrial and automotive environments, the internal environment of an aircraft can be highly dynamic, influenced by factors such as the phase of flight, internal configuration, and the activities of passengers, crew, and cargo [28] [34]. Given the criticality of aircraft functions, performance metrics are stringent and require thorough analysis during the design process. As WSNs typically consist of geographically dispersed communicating nodes, they are susceptible to various forms of cyber attacks, ranging from physical breaches to adversarial modes. In an aircraft context, there can be a mixed mode of attacks with a higher likelihood of adversarial actions, which may occur in a passive manner, such as eavesdropping, or through active methods like injecting malicious packets into the network [27] [35] [11].

2.3 Wireless Technology for Avionics

Even though wireless sensor networks (WSNs) have matured in industrial applications, significant research continues into adopting wireless technology for in-flight aircraft communication. The aerospace industry is consistently evaluating the feasibility of deploying WSNs. To address challenges that arise with wireless networks, such as interference due to radiation emissions in specific frequency bands, throughput issues, and other quality of service (QoS) parameters, there is potential to augment these networks with alternative technologies.

In paper [2], the need for wireless technology inside aircraft, along with its benefits and challenges, is analyzed. An approach towards Wireless Avionics Intra-Communications (WAIC) using 4.2 GHz radio is explained. Authors in [36] identify design issues of WAICs, spanning from physical-layer to application and security layers, using structural health monitoring (SHM) as an example. In the research [10], the authors present alternative architectural concepts and implementation strategies for WAIC at 2.4 GHz. [37] discusses the advantages of using ultra-wideband (UWB) technology over traditional wireless solutions within aircraft.

The work presented in [38] outlines an architecture for a next-generation WAIC network that incorporates reconfigurable intelligent surfaces (RIS) and focuses primarily on wideband (WB) and millimeter wave (mmWave) communications for WAIC systems. The authors explore the propagation characteristics of WB/mmWave WAIC channel models inside aircraft, as well as channel coding techniques, including low-density parity-check (LDPC) codes, specifically collective-encoded LDPC codes (CE-LDPC).

In the paper [39], an approach to developing a code division multiple access (CDMA)-based wireless sensor network for fire and gas systems is detailed. The paper [40] discusses the advantages and disadvantages of CDMA compared to carrier-sense multiple access (CSMA), frequency division multiple access (FDMA), and time division multiple access (TDMA) technologies for WSNs.

Additionally, Authors in [41] analyze the drawbacks of WSNs with MAC layer protocols based on IEEE 802.15.4 for low data rate communication, proposing a receiver-assigned code division multiple access (RA-CDMA) physical (PHY) layer multiple access technique. This technique may enable greater network scalability while maintaining performance and enhancing robustness. Furthermore, research [42] suggests a technique for combining CDMA with specific channel coding algorithms, such as Raptor codes. Lastly, in the research presented by [43], a theoretical framework is proposed for the accurate comparison of minimum energy coding in coded division multiple access (CDMA) wireless sensor networks.

As IAWSN/WAIC technology rapidly develops, researchers are encountering various challenges and continuously addressing them through ongoing research. Some literature provides insights into improving the Quality of Service (QoS) of IAWSN/WAIC by tackling interference issues and utilizing AI/ML to mitigate and resolve problems.

The paper [44] introduces a novel solution called 6TiSCH-CLX, designed

to meet stringent Quality of Service (QoS) requirements through cross-layer communication. This solution extends the 6TiSCH framework at both the network and Medium Access Control (MAC) layers, specifically addressing challenges related to latency and reliability, independent of the physical layer.

In another study, [45] examines the suitability of new Long Term Evolution (LTE) and Fifth Generation (5G) wireless technologies for low data rate Wireless Avionics Intra-Communications (WAIC) applications. The authors use analytical models and conduct experiments with Narrow-Band Internet of Things (NB-IoT) hardware to support their findings.

Furthermore, [46] evaluates various wireless communication techniques to determine their feasibility for use in WAIC systems. A significant barrier to ensuring reliable communication in this context arises from the operation of existing Radio Altimeter systems. Concerns regarding the potential impact of 5G on Radio Altimeter and WAIC operations, due to their usage of the same frequency band, have been raised by the GSMA, a global organization that unifies the mobile ecosystem to foster innovation and positive change [47]. The U.S. aviation industry group RTCA highlighted potential interference from 5G networks in a white paper. Prior to this, the U.S. Federal Communications Commission (FCC) spent four years examining the use of the 3.5 GHz band by 5G, including input from the aviation industry. They concluded that the technical regulations adopted for 5G C-band service, along with a 220 MHz guard band separating 5G networks from aviation operations, "are sufficient to protect [aviation] services in the 4.2-4.4 GHz band." The FCC's order also indicated that this guard band is double the width initially recommended by the aviation sector.

Additionally, the study [48] presents a model for an avionics compartment channel, fitting its fading distribution to a Rician distribution. Based on this model, an explicit expression for the Ergodic Capacity (EC) can be derived analytically. When the average Signal-to-Noise Ratio (SNR) is set at 15 dB and the bandwidth at 20 MHz, the maximum system arrival rate can reach 80 Mbit/s, which exceeds the maximum WAIC communication rate specified by the ITU-R.

Moreover, advancements in the industrial segment of Structural Health Monitoring (SHM) have brought to light fundamental issues concerning wireless communication in relation to non-destructive testing sensors (NDT) [49]. Developments in wireless technology across several critical areas are also discussed, including applications in aviation, wind turbine systems, and bridges.

Lastly, the paper [50] summarizes the preliminary results of using artificial intelligence (AI) tools in this emerging technology. The authors highlight various issues related to reliability, trust, interoperability, and latency that must be addressed before WAIC/IAWSN technology can be commercialized. They anticipate that AI will enhance the applicability of this technology, contributing to the realization of the concept of "fly-by-wireless."

2.4 Priority Queuing Model for Analysis of Network Traffic

WSN facilitates reduction in the use of wire harnesses in the aircraft and hence overcomes the associated complexities of weight, cost and efforts due to maintainability. However suitable protocols need to be formulated in order to realize wireless communications for aircrafts. These protocols need to address the challenges in terms of bandwidth allocation for devices, transmission power as well as interference. Research studies in [2] reveals initial survey of design specifications and issues involved in development of protocols for WSN. The wireless network should be designed considering the number of nodes connected and desired end-to-end delays based on the relative locations of high and low data rate transmitters. Another important design consideration could be the specifications for medium access control protocols. WSN design specifications are best defined by modeling and simulation of network elements and network traffic. Envisaged design parameters can be evaluated through analysis of network performance from model predicted QoS parameters like turnaround time, network throughput, and system response.

A number of working groups have put together the literature related to the need aspects of WSN. Some of the related references are discussed in this section. Large scale WSN models have been analyzed using queueing models in [27] [35]. Analytical Models of MAC protocols have been developed for performance evaluation as per [29] [30] [29]. The energy requirements and mobility aspects of WSN have been studied in [32] [33]

2.5 Security Architecture for WSN

A WSN inside an aircraft consists of a geographically distributed collection of communicating nodes located in the cockpit, cabin, cargo area, lavatories, wings, landing gears, and other sections. These nodes are susceptible to a variety of attacks, including both physical and adversarial threats. Attacks may occur in mixed modes, with a higher likelihood of adversarial techniques being employed either passively, such as eavesdropping, or actively, via the injection of malicious packets into the network.

Zou et al. [51] discuss the security strengths of existing industrial and enterprise wireless communication protocols, including WPAN, WMAX, LTE, and Bluetooth. They categorize attacks at the Physical (PHY) and Medium Access Control (MAC) layers of the network. Even with current security protocols in place, a significant challenge is achieving multi-objective optimization of security, reliability, and throughput, while still meeting the configurability and scalability requirements of the network. Security mechanisms for WSN should aim to maximize QoS under the specified reliability and throughput requirements of a WSN application. The primary metrics for assessing an attack can be defined as 1) Packet Delivery Ratio (PDR) and 2) End-to-End Delay (EED)

[52]. Wireless attacks, regardless of their mode, can impact one or both of these metrics. Therefore, it is crucial to evaluate a security protocol based on its effects on PDR and EED.

Park et al. [53] provide a survey and analysis of existing wired protocols, along with the potential benefits and challenges of adopting WAIC for aircraft applications. The authors highlight various security threats, including adversarial attacks, jamming attacks, man-in-the-middle attacks, and false alarms. In another survey, Yu et al. [54] discuss the benefits and challenges associated with the development and implementation of WAIC, focusing on wide-band (WB) and millimeter-wave (mmWave) communications.

The development of a security architecture for WSN comprises three broadly categorized design elements: 1) generation of security keys, 2) management of the keys throughout the operation of the network, and 3) extraction of keys at the receiving end. While standard encryption algorithms such as RSA, AES, and Elliptic Curve Cryptography (ECC) are utilized for enterprise and low-data-rate wireless applications, their applicability to power-constrained WSNs is debatable. Mansour et al. [55] present a review of standard security protocols like AES, analyzing their effectiveness in terms of computational efficiency and formal verification using the Scyther tool. Rifà-Pous et al. [56] offer a detailed analysis of the computational time and energy required to run standard security methods such as AES, hash functions, and ECC on low-energy devices. This comparative analysis directly impacts the delay and throughput requirements of real-time WSNs within an aircraft.

To optimize computing time, significant advancements have been made in the field of hardware-based encryption [57] [58]. Extensive research has also focused on security key generation and extraction at the physical layer. According to the literature, physical layer encryption can be classified and studied in three main categories:

(i) RSS-based strategies: Research [52], [55] emphasizes the need for optimized algorithms for key revocation and key generation using symmetric key cryptography. Furthermore, [56] highlights the advantages of hash chain functions and elliptic curve cryptography, while [58] discusses the use of multipath channels to enhance security performance in Two-Way Relay Networks. Additionally, [59] [60] propose methods for establishing keys based on the physical properties, such as signal strength fluctuations in a wireless channel, which are suited for peers with diverse computational resources.

(ii) Frequency selectivity-based strategies: Research [61], [62] suggests that due to the reciprocity between a transmitter and a receiver, they can share one-time information about their fluctuating channel. This enables a secret key agreement scheme without the need for key management and distribution processes.

(iii) Channel impulse response-based strategies: A survey by [63] reviews encryption techniques that utilize channel characteristics. The security of these schemes is based on the reciprocity principle [64], which states that channel fluctuations can provide a source of common randomness for two communicating peers, making it difficult for eavesdroppers to measure these fluctu-

ations. Research by [65] explores the generation of random numbers using the physics associated with multipath propagation and multiple antennas to establish secure encryption keys between two wireless nodes. Moreover, [66] investigates both theoretical and practical approaches for key generation that exploit reciprocal MIMO channel fluctuations. In addition, [67] analyzes the performance of the CQG protocol (Channel, Quantization, and Guard band), yielding closed-form expressions for bit error rate (BER) and key generation efficiency. Lastly, [68] presents an intelligent method for key extraction that employs guard intervals to separate decision regions.

Several other approaches have also been proposed for secret key generation, such as reverse pilot signaling for OFDM transmission in wireless systems [69] and bit error rate fluctuation [70]. The Chinese Remainder Theorem is discussed in [71] and [72], while reactive jamming methods are explored in [73] and [74]. The shortcomings of physical-layer (PHY) based secure key generation have been reported in [75]. Techniques based on Received Signal Strength (RSS) are suitable only for pairwise key generation, whereas frequency selectivity approaches often fail to provide sufficient entropy in practical RF environments. Additionally, channel impulse-based techniques require advanced channel estimation and time synchronization, which may not meet the throughput requirements and delay constraints for wireless sensor networks (WSNs) deployed in aircraft applications. PHY-based secure key generation often faces challenges, including interference, path loss, multipath channel fading, and link failure [76].

A WSN security policy utilizing group-based key management and identity-based cryptography has been presented in [77]. This research demonstrates how to specify and implement a new group-based security policy using trust and risk as two key factors that influence the behavior of sensor nodes. The security policy operates on an abstract representation of sensor node components, transactions, and connections. The trust function determines the degree to which one group of nodes shares keys with its neighbors, while the risk function assesses the impact of a particular transaction on the network. Decisions regarding actions are made based on the combined trust and risk values calculated for the corresponding action. This security policy has proven effective against node replication and Sybil attack modes. However, processing times on 32-bit Smart MIPS architecture microprocessors are around 290 milliseconds. Computing time improves with Intel processors operating at 400-416 MHz, but this comes at the expense of increased energy consumption. Secure Group Communication (SGC) has been studied in detail [78] and can be effectively implemented with robust key and membership management for various groups communicating with one another. Nevertheless, current SGC methods still face deployment challenges in WSNs, including resilience against compromised nodes, computational efficiency, message overhead, and transmission energy loss.

An effective security architecture for WSNs requires efficient key management techniques. An extensive review of wireless sensor network key management is presented in [63], discussing both symmetric and asymmetric key

management methods in detail.

Symmetric key management is generally considered to be superior to asymmetric methods when it comes to processing time and energy consumption. Although asymmetric algorithms offer greater security strength, symmetric methods are typically limited to high-end processing units. Intra-aircraft wireless sensor networks (WSNs) often face resource constraints, necessitating the development of optimized security algorithms that provide greater strength while reducing overhead.

We propose a hybrid security scheme where key establishment occurs within network elements (such as network managers and data managers) that do not have power limitations, while only symmetric key operations are carried out on the sensor nodes. A survey of distributed key management algorithms has been previously reported [79].

Our classification of key management schemes includes a detailed discussion of performance metrics that evaluate factors such as security, efficiency, and reliability. We provide an in-depth trade-off analysis that considers the relationship between security and computational efficiency. It is ultimately suggested that combining the metrics of public and symmetric methods offers a promising approach. Lee et al. [80] present a comprehensive description of operational metrics for comparison, including scalability, robustness, and reliability in dynamic key management schemes. We identify three key distribution schemes: Network-based, Pairwise, and Group-based methods. The trade-off between computational efficiency and robustness is proposed as a critical factor in designing security protocols for wireless sensor networks.

The methods discussed thus far are specific to certain use cases and do not provide a comprehensive solution for secure communications within intra-aircraft WSNs. In this thesis, we address this gap by presenting a security architecture that outlines algorithms for key generation, key distribution, and key revocation. We utilize symmetric key cryptography and implement a group-based policy for key distribution and management. Our security algorithms have been optimized concerning packet delivery ratio (PDR) and end-to-end delay (EED) metrics [52], in addition to minimizing computing and transmission overhead. We have evaluated the proposed security architecture on a physical prototype to assess its effectiveness in meeting the desired network performance requirements.

2.6 Applications of IAWSN

IAHM-related applications enable aircraft to acquire data from various systems and subsystems, analyzing it to reach critical decision-making points. Researchers have identified multiple application areas in this field of study [81].

2.6.1 IAWSN Architecture for IAHM

IAHM hosts applications such as prognostics and diagnostics that facilitate condition-based maintenance [82] for systems and subsystems. In safety-critical domains like aerospace, IAHM must support fault-tolerant responses, including system and subsystem reconfiguration, to prevent catastrophic failures. Additionally, it aids in planning and scheduling post-operational maintenance [83], which helps prevent sudden field failures.

A comprehensive list of proposed applications is provided, covering internal components of the aircraft as well as its external structure. These applications are designed to handle variable data rates and data types from a large number of sensors [81]. A standard architecture for the flow of information within a highly integrated health monitoring system is outlined in [84].

IAHM must also process a vast amount of heterogeneous data—up to terabytes in size—necessitating advanced data mining capabilities [85]. The Integrated Modular Avionics (IMA) architecture discussed in the literature utilizes a wired network for clustered communication.

2.6.2 IAWSN Architecture for WPT

A significant amount of research has been published in the literature focusing on solutions for drones, UAVs, and related applications. Below are several references that discuss the evolution of technologies for Wireless Laser Power Transfer (WPT) methods.

One study [86] theoretically investigates the feasibility of a laser-based wireless power transfer mechanism for drone applications, aiming to increase their operating time. The authors conclude that drones can be charged wirelessly during operation at considerable distances with acceptable efficiency. They evaluated laser-based photovoltaic materials, including GaAs, CdTe, and c-Si PV, and found that the WPT system can approximately receive net powers of 73.5 W, 62.6 W, and 33.2 W at a distance of 500 meters.

Another research study [87] examines wireless power charging methodologies for unmanned aerial vehicles (UAVs) in three categories: (1) Near field, (2) Far field, and (3) Solar-powered UAVs, all aimed at enhancing flight endurance. The research on Laser Power Transfer (LPT) is driven by the need to remotely power UAVs, satellites, and other mobile electric devices. An overview of LPT technology, focusing on optimizing efficiency, is presented in [88].

Additionally, [89] discusses the necessity and feasibility of Optical Wireless Power Transfer (OWPT), emphasizing its importance in supplying power to Internet of Things (IoT) terminals and the impact of dynamic OWPT. This study highlights several OWPT techniques, including optical beamforming, distributed laser charging (DLC), adaptive-DLC (ADLC), simultaneous lightwave information and power transfer (SLIPT), Thing-to-Thing (T2T) OWPT, and high-intensity laser power beaming (HILPB).

Research in [90] analyzes the High Intensity Laser Power Beam (HILPB) across various scenarios and discusses performance parameters, recommend-

ing the design of more robust receivers. [91] presents a review of LPT, demonstrating the basic concepts of photoelectric emitters, transmission channels, and receiver materials. [92] discusses systems, circuits, and standards for sensor-based applications.

While much of the literature primarily addresses drones and UAVs, few studies have focused on wireless power transfer within aircraft. In [10] and [2], the authors explore strategies for implementing wireless intra-aircraft communication.

2.7 Aviation Standards and Certifications

AVSI is a cooperative research environment that includes major aerospace companies, government organizations, and academic institutions working together to address common challenges faced by its members. To this end, AVSI helped establish a special committee and working group responsible for developing WAIC standards, which guided the production and integration of WAIC applications [81]. These experts ensured that spectrum usage complied with International Civil Aviation Organization (ICAO) convention guidelines to facilitate equipment certification. The two main panels involved are RTCA SC-236 and EUROCAE WG-96 [7], which set the primary minimum operational performance standards (MOPS) requirements [8].

Under AVSI project AFE 76 — WAIC Protocols, comprehensive network and hardware architectures, protocols, requirements, and appropriate protection criteria for spectrum sharing are being defined. This aims to safeguard WAIC and legacy altimeter systems from interference. WAIC applications are categorized as either Low Rate (data transmit rate < 10 kbits/sec) or High Rate (data transmit rate > 10 kbits/sec), each with distinct size, weight, and power (SWaP), cost, and performance requirements. AFE 76 addresses more detailed design issues, including system boundaries for the application of WAIC standards, plans for WAIC spectrum assignments to ensure efficient usage, and the development of a channel allocation and channel spacing scheme for WAIC systems.

EUROCAE WG-96 has developed a MOPS for a WAIC component that enables WAIC systems to safely coexist with radio altimeters in the frequency band of 4200–4400 MHz.

SC-236, titled ”Standards for Wireless Avionics Intra-Communication System (WAIC)” within the 4200-4400 MHz band, established MOPS for wireless equipment, facilitating spectrum sharing between WAIC systems and other aviation systems. Its objective is to support procedural planning and decision-making for the FAA and the aviation community [6].

OSA-CBM has established guidelines for developing architectures for Condition-Based Monitoring of Commercial Aviation Systems [84].

SAE documents ARP 4754 and ARP 4761 [93] provide guidelines for the development of civil aircraft and systems. However, the working groups are evolving guidelines specifically for IAWSN/WAIC implementation. Clear

guidelines for IAWSN/WAIC implementation are still developing alongside the maturation of the technology.

2.8 Research Gaps

Based on the survey presented in earlier sections, we have identified the following research gaps:

1. There is currently no tested and recommended wireless sensor network (WSN) architecture that enables seamless communication while meeting the performance requirements of next-generation aircraft, particularly for real-time health monitoring applications.

2. There are significant technological challenges in achieving the necessary throughput for WSNs, which must handle variable data rates and types throughout all phases of flight in the resource-constrained environment onboard aircraft.

3. The IEEE 802.15.4 protocol faces difficulties in meeting the performance requirements of Integrated Aircraft Wireless Sensor Networks (IAWSN) due to the coexistence of various networks and sources of interference in the cockpit and cabin environment.

4. Most existing literature focuses on secure wireless networks for industrial and process applications. Although these studies identify opportunities and challenges for adapting such frameworks to aircraft applications, there is a noticeable gap in the development and implementation of effective security solutions for wireless networks within aircraft.

2.9 Chapter Summary

In this chapter, we present a comprehensive review of the literature concerning various aspects of sensor networking in aerospace, industrial, and process applications. We analyze the performance requirements for sensor networks in complex avionic systems, focusing on feasibility, scalability, reliability, interoperability, safety, and operational considerations, all in the context of meeting regulatory and certification standards. Additionally, we identify potential gaps in the industry, which we see as opportunities to address in this research work.

Chapter 3

Architecture of Intra-Aircraft Wireless Sensor Network

3.1 Introduction

Wireless sensor technology has emerged as a significant advancement in modern aviation, presenting opportunities to enhance design efficiency, reduce system weight, and optimize performance. As the aerospace industry increasingly adopts these advanced systems, it must navigate crucial considerations related to reliability, compliance with stringent safety standards, and seamless integration with existing infrastructures. Currently, most avionics buses utilize local area networks based on industry-specific standards, such as ARINC 429, AFDX (ARINC 664), MIL-STD 1553, and CAN [16]. However, the reliance on wired networks introduces challenges related to scalability and adaptability, as well as increased time and costs associated with meeting regulatory and certification requirements due to their fixed architecture.

In this chapter, we have presented a trade study of wired and wireless sensor networks.

1. We have compared various sensor types, interfaces, applications, corresponding Line Replaceable Units (LRUs), LRU interfaces, communication protocols, network architectures, and certification requirements essential for aerospace applications.

2. We have analyzed the benefits and challenges of these sensors and established the role of Wireless Sensor Networking (WSN) as a transformative technology in the future of aviation.

3. We have proposed using WSNs on board aircraft as an alternative to existing wired networks.

4. We have outlined an approach for designing a robust, secure, adaptable, and scalable WSN while addressing the associated design challenges.

5. We have proposed a methodology to integrate various sensor-based applications for the Intra-Aircraft Wireless Sensor Network (IAWSN) operating in the ISM band, which can be expanded to Wireless Avionic Intra-Communication (WAIC) that operates in the 4.2 GHz - 4.4 GHz spectrum.

6. We have also evaluated various architectural concepts to determine their applicability within aircraft. These concepts include:

   (a) Open-loop monitoring and displaying aircraft operational status and the health status of aircraft components,

   (b) Implementation of onboard analytics for prognostics and diagnostics and

   (c) Recommendations for data-driven decision-making for pilots and crew.

3.2 Trade Study of Sensor Network

Present Scenario: The Figure 3.1 depicts the distribution of various wired sensors throughout the aircraft. While it does not include all sensors, it illustrates the considerable amount of wiring needed, which is significantly high. As the number of sensors and the size of the aircraft increase, the wiring demands multiply even further. This extensive wiring contributes to the aircraft's overall weight and leads to operational inefficiencies due to increased fuel consumption. Most of the sensors are wired, making reconfiguring or relocating them challenging. These sensors are spread across the aircraft, both externally and internally, resulting in hundreds of kilometers of wiring within the aircraft. This situation also complicates maintenance and servicing, as it adds complexity to replacing sensors.

Interface Technique for Wired Sensors: It is important to understand the various types of wired sensors, as well as their current interface techniques and measurement methods. Sensors and sensor network applications can be classified based on their location and data rate. The data rate is categorized as either High (H) or Low (L), while the location can be classified as either Inside (I) or Outside (O) of the fuselage. Table 3.1 presents a list of different sensors along with their interfaces to the signal processing unit, measurement techniques, and digital communication methods used after signal processing. Additionally, the table classifies each sensor based on its operating data rate and location.

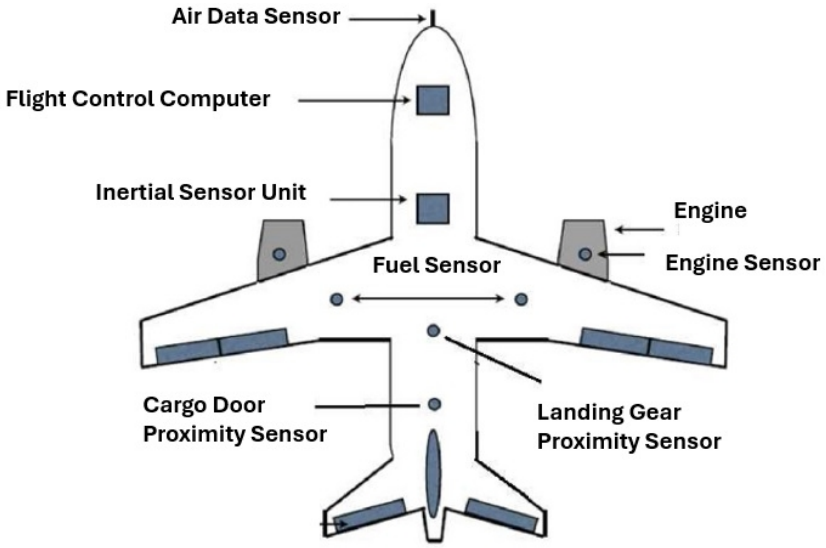


Figure 3.1: Aircraft Sensor Configuration

Type of Sensor	Interface	Measurement Technique	LRU to System/Subsystem Interface	Type of Sensor
Fuel	Excitation - Response [1]	DC or AC Capacitance	ARINC429	LI
Proximity	Drive Sense (1 Wire for Drive and 1 Wire for Sense)	Inductance	Discrete	LI & LO
Engine (Vibration, Temp)	2-Wire or 4-Wire	Resistance	Discrete	LO
Temperature Sensors	2-Wire or 4-Wire	Resistance	Discrete	LI & LO
Air Data - Pressure[2]	Static Port on body of Pilot Probe	Solid state Sensing	ARINC429	LO
Air Data - Temperature[3]	2-Wire or 4-Wire	Resistance	ARINC429	LO

[1] - 1 wire for excitation and 2 wires for response.
[2] STAP - Static and Total Air Pressure
[3] SAT / OAT - (SAT - Static Air Temperature), (OAT - Outside Air Temperature) Bluetooth speeds at various versions - 721 Kbps (1.0),
LI - Low data rate and Internal to Fuselage
LO - Low data rate and External to Fuselage

Table 3.1: Aircraft Sensor Interfaces

Interfaces of Wired LRU/Processing Unit in Aircraft: Below is a list of typical wired interfaces used by various Line Replaceable Units (LRUs) for communication with other systems and subsystem components:

1. ARINC 429
2. ARINC 717 (Bipolar& Biphase)
3. MIL-STD-1553
4. JIAWG
5. Fibre Channel
6. IEEE 1394 (FireWire)
7. ARINC 664 (AFDX)
8. CAN

Benefits and Drawbacks of Wired Sensors: Wired sensors provide a dependable means of communication, and avionics systems have successfully used them for many years. Over time, various standards for digital communication and sensor interfaces have been developed and implemented. However, one significant drawback of wired sensors is the additional weight they add to the aircraft, which can negatively impact performance by reducing fuel efficiency. Safety concerns also arise due to issues like stray capacitance, and electromagnetic interference (EMI) becomes a critical factor, encompassing both emissions and susceptibility. The effects of EMI and the necessity for effective noise management demand sensitive signal conditioning in the processors. Additionally, routing cables within the aircraft can be challenging given its shape and limited space. The aircraft's mechanical structure imposes restrictions on cable routing, complicating installation. The requirements for sensitive signal conditioning and various shielding measures for the wires contribute to increased costs and weight, ultimately outweighing the benefits of using wired sensors.

Various drawbacks of wired sensors discussed in the previous section necessitate the exploration of better alternatives. One possible solution is to replace many of an aircraft's wired interconnections with wireless network. This approach can provide several benefits, including weight reduction, easier maintenance, faster aircraft design, simpler retrofitting, and greater redundancy. Wireless sensors offer several advantages over wired sensors, including reduced installation and maintenance time and costs throughout the equipment life cycle, lower weight, enhanced reliability, and easier maintenance. Adding redundancy to a wired configuration increases weight and installation complexity, while a wireless solution simplifies adaptation by only requiring the addition of wireless sensors.

The advantages of wireless sensors discussed above facilitate a comparative analysis of the various wireless technologies and standards available. Wireless

	WiFi IEEE 802.11a	**WiFi IEEE 802.11b**	**WiFi IEEE 802.11g**	**WiFi IEEE 802.11a**	**ZigBee IEEE 802.15.4**	**Bluetooth IEEE 802.15.1**	**NFC**
Data Rate	54 Mbps	11 Mbps	54 Mbps	100 Mbps*	20 Kbps to 250 Kbps	721 Kbps to 1 Mbps**	106, 212 or 424 Kbps
Frequency Band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5 GHz	868 MHz or 2.4 GHz	2.4 GHz	13.56 MHz
Modulation	OFDM	DSSS	OFDM, DSSS	OFDM	DSSS	FHSS	ASK
Licensed	NO	NO	NO	NO	NO	NO	NO

* Data rates up to 600 Mbits are achieved only with the maximum of four spatial streams using a 40 MHz-wide channel.
** Bluetooth speeds at various versions - 721 Kbps (1.0), 3 Mbps (2.0), 24 Mbps (3.0), 1 Mbps (4.0) (Low Energy)

Table 3.2: Wireless Sensor Technologies

Wired Communication Interface of LRU	Data Rate Type	Data Rate	Possible Wireless Solution Protocol	Power Consumption
ARINC 429	Low	12 KHz → 100 KHz	ZigBee	Low
ARINC 717 Bipolar	Low	384 Hz → 98 KHz	ZigBee	Low
ARINC 717 Biphase	Low	384 Hz → 98 KHz	ZigBee	Low
MIL 1553	Medium	1 MHz	WiFi	High

Table 3.3: Replacement of Wired with Wireless Sensors

operations enable services such as long-range communications. Table 3.2 lists the various wireless technologies that can be considered for communication inside aircraft. This table serves as a high-level summary of the comparative study of these wireless technologies.

Table 3.3 examines the feasibility of communication channels based on data rates and physical constraints. Among the options, ZigBee stands out as the most beneficial standard because it is specifically designed for wireless sensor networks and operates at much lower power levels than the alternatives. If all sensors on the aircraft are battery-powered, ZigBee offers significant flexibility in terms of placement and upgradability.

Feasibility Consideration - Key Factors: The previous discussion on wireless technologies, sensor and line replaceable units (LRUs) interfaces, and sensor network topologies highlights several essential factors for the avionics industry. This section focuses on a few critical considerations for wireless applications in aircraft. A preliminary study is presented to review the various feasibility factors that should be evaluated before choosing a wireless alternative.

Selection of Protocols: Data integrity is a key factor in the protocols used in the aviation industry. High-reliability data communication without data loss is critical for the safety systems developed in this sector. With wireless sensors and LRUs, it is essential to implement communication protocols that address these data integrity needs. Existing wireless protocols may require modifications to ensure highly reliable data communication over wireless media. some possible improvements include adding additional cyclic redundancy check (CRC) bits, implementing software checks, and creating new protocols with larger CRC values. A few extra CRC bits can significantly reduce the risk of failure modes.

Design Driver	Requirements Definition
Scalability	Support addition and removal of end devices communicating in the network
Configurability	Support different data formats, interfaces, data rates and priorities for the end devices
Complexity	Low network setup and lost node reconnect time, easy maintenance and debugging

Table 3.4: Design Drivers and Definition of Architectural Requirements

3.3 Wireless Sensor Network Inside Aircraft

Wireless communications within an aircraft face several design challenges due to the need to support a large number of devices, including sensors, avionics and actuators, that exchange data in various formats. Data must be transmitted within specified delivery deadlines while achieving the desired throughput. The radio environment inside the aircraft is subject to interference from spurious RF signals originating from multiple sources, such as Wi-Fi and Bluetooth devices. This interference can disrupt the IAWSN, leading to data corruption or loss. Therefore, the proposed IAWSN architecture focuses on the key design drivers outlined in Table 3.4.

The architecture of the wireless network is selected to support three key aspects: (1) scalability, (2) configurability, and (3) complexity. The first two aspects address the requirements of next-generation avionic applications, which will need to integrate a large number of diverse sensors and management systems in future aircraft. The third aspect, complexity, emphasizes the importance of flexibility in network deployment and troubleshooting.

3.3.1 Concept Analysis for Selection of Architecture of IAWSN

The architecture of the IAWSN is chosen through a comprehensive trade study of different architectural concepts. This trade study process involves defining use case scenarios and environmental parameters, identifying design drivers, and developing multiple architectural options. Figure 3.2 illustrates the architecture selection process for the WSN, while Table 3.5 presents a sample trade study for the architecture options.

3.3.2 Network Architecture

A typical deployment of the network inside an aircraft is shown in Figures 3.4 and 3.2. The wireless network architecture consists of the following elements.

1. Nodes – sensors, actuators, avionics elements, data managers and network managers communicating over wireless links.
2. Data Managers (DM) – routers or aggregators that communicate with the nodes on wireless links.

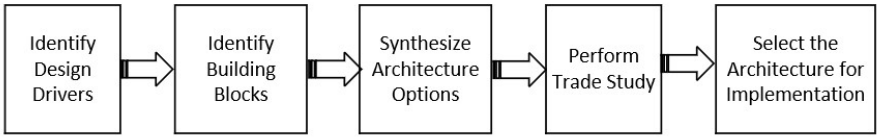


Figure 3.2: WSN Architecture Selection Process

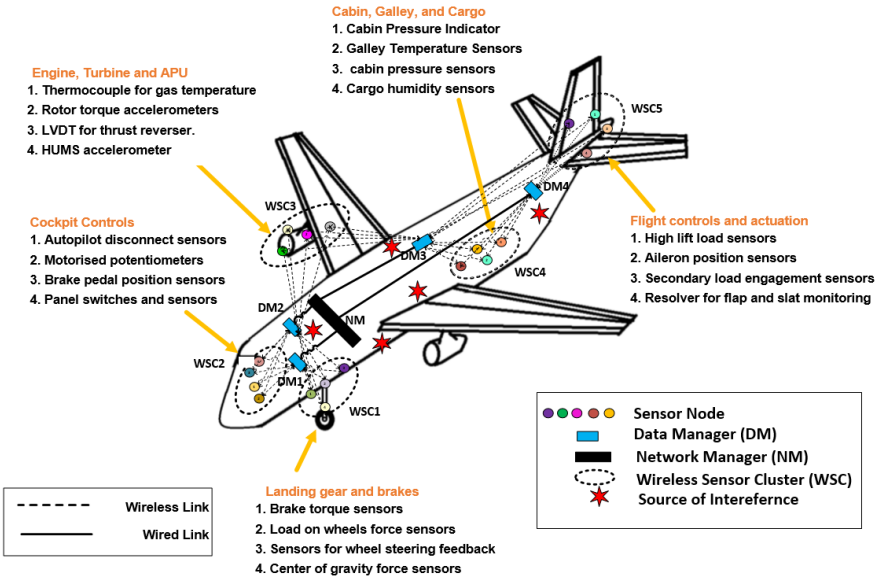


Figure 3.3: Architecture of the Proposed Intra-Aircraft Wireless Sensor Network

3. Network Manager (NM) – embedded processing unit with high-performance computational resources and memory and multiple interfaces.

In this architecture, nodes communicate with data managers via wireless links, while the data manager connects to the network managers through a wired medium.

The wireless sensor network within an aircraft must be scalable and configurable, especially concerning the nodes. This is essential due to the possibility of an increase in both the number and variety of sensors and avionics. Once installed, data managers typically cannot be replaced until they either fail or reach the end of their operational lifespan.

Given that the number of data managers is significantly smaller than the number of nodes in the network, the topological complexity of wired communication between the data managers and the network manager is lower compared

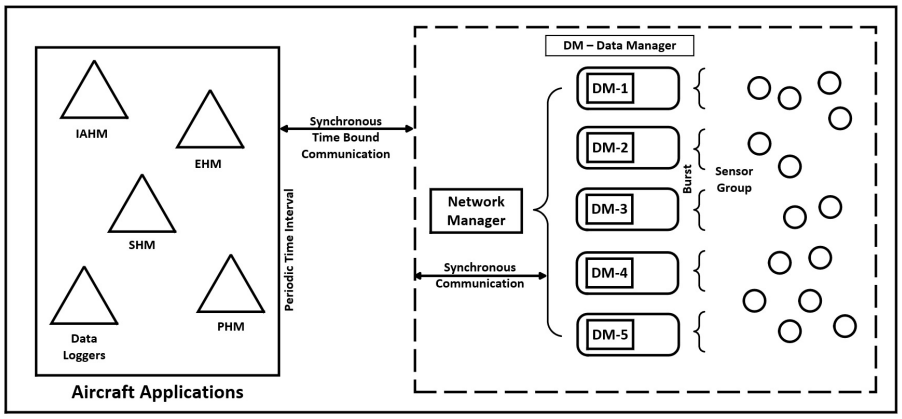


Figure 3.4: Typical Sensor Network Entities: Network Manager, Data Managers and Sensor Cluster.

to the wireless communication between data managers and the nodes. We have conducted a detailed trade study of functional elements based on the design drivers and performance parameters and proposed a hybrid communication topology to meet the design objectives outlined in Table 3.5.

3.3.3 Design Features

Node Association and Data Clusters

The topology of the IAWSN enables distributed data communication between network nodes and the network manager through data managers. Depending on the wireless communication range, signal strength, and link quality parameters, nodes may associate with a specific data manager located nearby. This results in the formation of logical data clusters, where each data manager receives information from multiple associated nodes on different frequency channels. The data is consolidated at the data manager and relayed to the network manager upon request from the applications.

3.4 Communication Protocol Selection

Short-range wireless communication protocols such as IEEE 802.15.4, IEEE 802.11 (Wi-Fi), and Bluetooth LE are well-suited for intra-aircraft communication applications, given the relatively short distances between aircraft systems. IEEE 802.15.4 is ideal for low-power, low-data-rate wireless networks, whereas IEEE 802.11 is appropriate for medium-range, high-throughput applications. Bluetooth LE is commonly used for short-range device-to-device communication. In the context of aircraft system health monitoring applications, which is

Design Driver	Description of Design Drivers	Weight	Rating		Likert Score	
			D1	D2	D1	D2
Architecture Simplicity - 20%	**Software Complexity** 1. Computational Complexity of Message Sequencing and Fault Tolerance Algorithms	7%	5	1	0.35	0.07
	Hardware Complexity 1. No. of Hardware components and Network Entities 2. Module Interfaces 3. Wired Connections	7%	5	5	0.35	0.35
	Control Flow Complexity 1. Association and network setup mechanisms (High) 2. Switching to redundant coordinators from master coordinator (Medium) 3. Handshaking and Timing Signals between network entities (Low)	6%	5	3	0.3	0.18
Hardware Cost - 20%	No. of types of hardware modules and physical interfaces	20%	5	5	1	1
Network Reliability - 36%	Fault Tolerance of WRDC	30%	5	5	1.5	1.5
	Probability of loss of packets from sensor nodes	5%	3	5	0.15	0.25
Network Initialization Time - 10%	Initial configuration time	8%	5	4	0.4	0.32
	Restructuring nodes	2%	5	4	0.1	0.08
Channel Budget - 15%	Software Complexity	15%	5	2	0.75	0.3
Total		100%			4.9	4.05

Table 3.5: Trade Study on Wireless Network Architectures

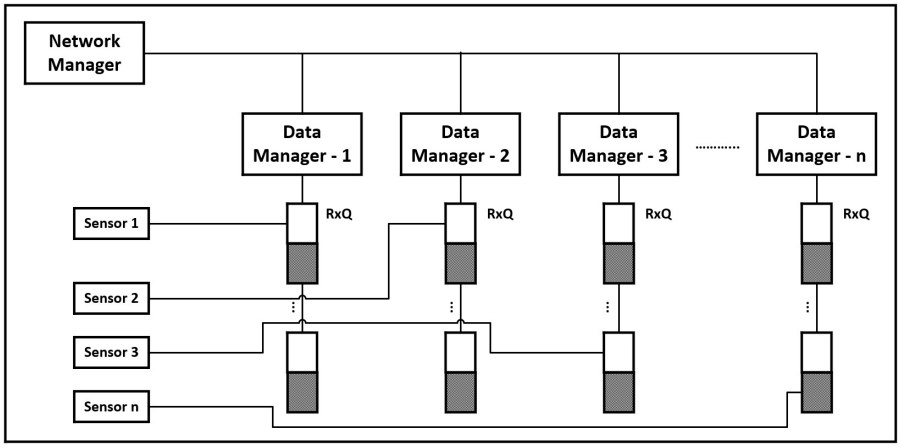


Figure 3.5: IAWSN and Buffering Scheme at the Network Manager for Achieving Asynchronous Communication with Multi-Rated Nodes (shown as sensors).

the primary focus of this research, large-scale networks consisting of many sensor nodes across multiple clusters will be necessary. Therefore, IEEE 802.15.4 is a strong candidate for IAWSN, due to its low power consumption.

3.4.1 IEEE 802.15.4 Protocol and Radio

IEEE 802.15.4 is a standard for low-rate wireless personal area networks (WPANs) that is widely used in industrial automation, home automation, and sensor networks. This standard defines the physical and media access control (MAC) layers for low power and low data rate wireless devices. These devices operate in the unlicensed Industrial, Scientific, and Medical (ISM) bands, specifically at frequencies of 868 MHz, 915 MHz, and 2.4 GHz. Among these options, devices operating in the 2.4 GHz band provide the highest throughput, making them the preferred choice for IAWSN. A typical IEEE 802.15.4-based wireless device has specific design specifications.

- Operates in 2.405 to 2.480 GHz frequency range
- 16 channels each with a total bandwidth of 5MHz – 2 MHz main band and 3 GHz guard band
- Maximum throughput 256 kbps
- Media Access Control – CSMA, TDMA

MAC Layer: The IEEE 802.15.4 Media Access Control (MAC) layer is designed to be versatile, accommodating both synchronous and asynchronous communication, as well as supporting mesh and star topologies. This protocol

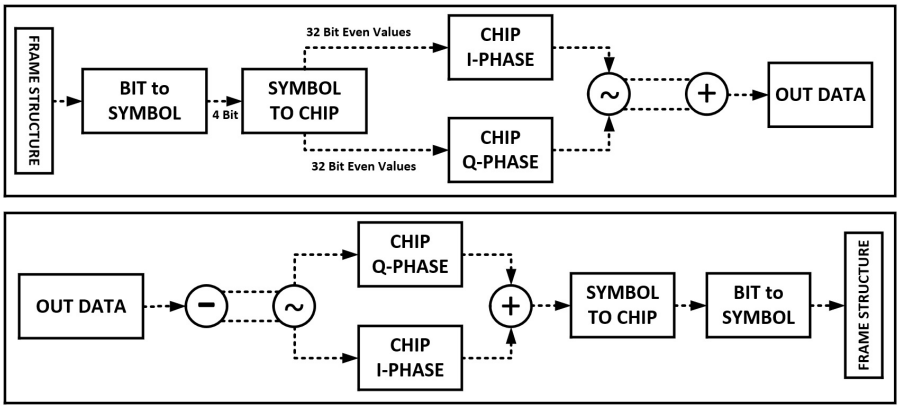


Figure 3.6: IEEE 802.15.4 Transceiver-Receiver

utilizes Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) for asynchronous multiple access. Additionally, it can be time-slotted to create a hybrid Time Division Multiple Access (TDMA) network. One significant concern regarding the IEEE 802.15.4 MAC layer is the unreliability caused by its contention mechanism. This issue becomes particularly problematic in highly dense and collision-prone networks [42].

PHY Layer: The IEEE 802.15.4 standard offers six PHY layer options, based on their requirements for frequency range and data performance. Four of these options utilize frequency hopping techniques known as Direct Sequence Spread Spectrum (DSSS), which enhance the signal's immunity to narrow-band noise and interference. The transmitter and receiver baseband processing chains for the IEEE 802.15.4 offset quadrature phase-shift keying (O-QPSK) PHY operating at 2.4 GHz using DSSS are illustrated in Figure 3.6. The O-QPSK PHY incorporates a 16-ary quasi-orthogonal modulation technique. During each data symbol period, four information bits are used to choose one of 16 nearly orthogonal pseudo-random noise (PN) sequences for transmission. These PN sequences are concatenated for successive data symbols, and the combined chip sequence is modulated onto the carrier using O-QPSK. The O-QPSK modulated signal is then passed through a half-sine pulse shaping filter before being sent to the transmitter's front end [94]. This mapping of the symbols to orthogonal chip sequences spreads the signal across a wider frequency band, improving its immunity to narrow-band noise caused by interference from other wireless devices operating on overlapping channels. The reverse process is executed at the receiver end to retrieve the transmitted data.

The IAWSN communication protocol is based on the IEEE 802.15.4 wireless protocol and is designed to support both synchronized communication for con-

trol applications and asynchronous communication required for event-based applications, such as aircraft health monitoring. Synchronized communication between the network manager and the applications is established by sending data requests to the data managers at regular time intervals. The data managers respond to these requests from the network manager in a synchronous manner. In contrast, asynchronous communication between the wireless nodes and data managers is facilitated through a dynamic buffering mechanism incorporated in the management software, as illustrated in Figure 3.6. The nodes transmit data to their respective data managers in each cluster, represented by sensors. The data managers store the received data in dedicated receive queues (RxQ). Subsequently, the network manager retrieves data from the data managers in a first-in, first-out (FIFO) manner. By utilizing data buffers within the data manager, communication between the data managers and the wireless nodes ensures zero data loss, even when data from fast nodes arrives before data from slower nodes. In addition to the core requirements outlined in Table 3.4, the proposed wireless architecture includes features for reducing electromagnetic interference and enhancing communication reliability. This is achieved through (1) synchronized channel management and (2) fault tolerance to ensure reliable data transfer.

3.5 Fault Tolerance

The architecture incorporates fault tolerance through redundant data managers and wireless channels to ensure uninterrupted communication between wireless networking entities, such as nodes and data managers. This fault tolerance is achieved through two levels of redundancy: (1) spatial redundancy, which refers to the physical locations of primary and backup data managers, and (2) spectral redundancy, which utilizes multiple backup channels available within the spectrum.

3.5.1 Spatial Redundancy

Spatial redundancy is implemented by assigning at least one backup data manager to each node cluster. According to the redundant association scheme, nodes within the cluster connect to the primary data manager when the network begins operating. If the connection to the primary data manager is disrupted, the node will automatically switch to the designated backup data manager. Identifiers for both the primary and backup data managers are assigned to each node cluster using a deployment matrix (see Table 3.6).

3.5.2 Spectral Redundancy

Data managers are configured to communicate with nodes through two channels: the primary channel and the secondary channel. During the network configuration phase, as described in the section 3.5.3-Channel Management,

Deployment Matrix						
Short Address	**IP Address**	**Data Rate**	**Primary Data Controller ID**	**Secondary Data Controller ID**	**Primary Channel**	**Standby Channel**

Table 3.6: Structure of a Deployment Matrix used to Configure the Wireless Network

the network manager automatically selects these channels. By default, data managers communicate with the nodes on the primary channel within the allocated spectrum. Suppose there is a loss of connection on the primary channel due to interference, poor signal quality, or failure of the corresponding radio module. In that case, the nodes will switch to the pre-designated secondary channel to ensure uninterrupted communication. The primary and secondary channels are predefined in the deployment matrix and are managed by the network manager. Each of these channels are, in turn, configured with 2 controllers each - primary and secondary controllers, which are segregated by their frequency of operation. Thus the architecture supports 2 logical backups (redundant controllers) in each one of the channels. channel In the event that communication is lost on the primary channel, the nodes will attempt to connect with the primary controller on the secondary channel. If communication fails even on the secondary channel, the nodes will then try to communicate with the secondary controller on the Primary channel. They will attempt to associate with the secondary controller on the secondary channel if that also fails. The node will enter idle mode if communication is lost with the secondary controller on the secondary channel.

The fields of the deployment matrix are as follows:

1. Short Address – node identifier used by Data Managers to communicate in the N/W.
2. IP Address – the logical network address of the node Data Rate – rate at which data is transmitted from the node
3. Primary Data Manager ID – network identifier for the Primary Data Manager
4. Standby Data Manager ID – network identifier for redundant Data Manager
5. Primary Channel – primary channel for communication
6. Standby Channel – redundant channel for communication

Figure 3.7 illustrates the operation of the fault tolerance mechanism, which utilizes interchangeable spatial and spectral redundancies. Spectral redundancy takes precedence over spatial redundancy.

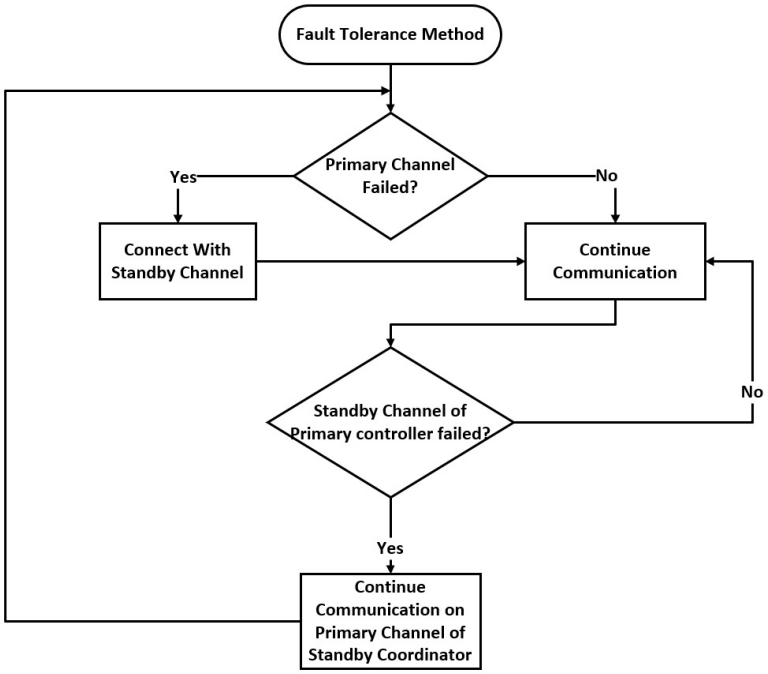


Figure 3.7: Flowchart of Fault Tolerance Mechanism

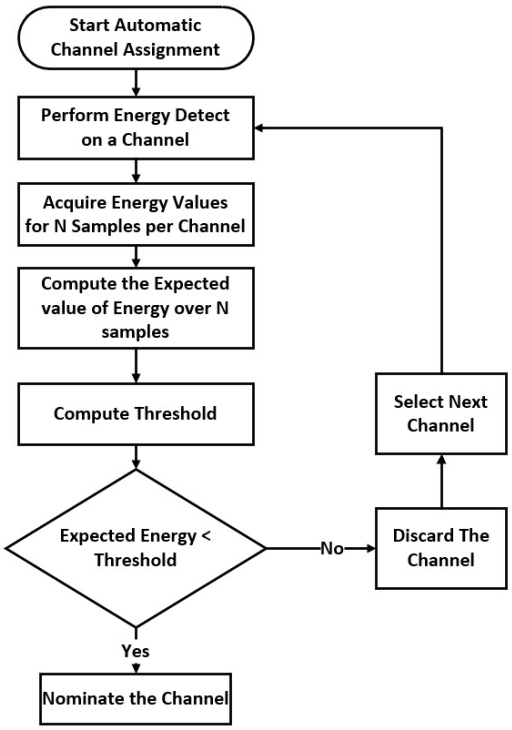


Figure 3.8: Automatic Channel Selection

3.5.3 Channel Management

The proposed IAWSN architecture effectively manages channels by using channel state estimates obtained at regular intervals. Data packets that share the same channel are multiplexed in time, enhancing throughput and optimally utilizing the available bandwidth. In an aircraft environment, where interference from other wireless devices is common, selecting the appropriate channels to achieve optimal communication performance for the IAWSN is essential. To address this issue, a scheme (illustrated in the flowchart of the Figure 3.8) has been developed to automatically identify the best channels for IAWSN communication within a specific RF (Radio Frequency) environment. This algorithm performs a comprehensive scan of the RF bands inside the aircraft, utilizing data managers to determine the optimal radio channels for the sensor network through an analytical approach.

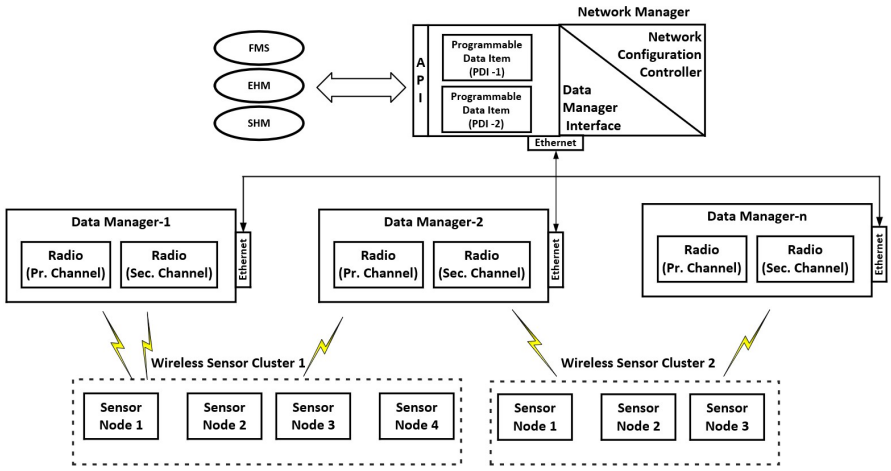


Figure 3.9: Integration of Sensor Applications with IAWSN

3.6 Integration of Sensor Applications with IAWSN

The IAWSN architecture is designed to support a wide range of aircraft applications that utilize various sensors and data types. For airlines and aircraft OEMs (original equipment manufacturers), integrating sensors and applications with the IAWSN should be a straightforward process that requires minimal costs and effort. To achieve this goal, it is essential to establish a standard set of application programming interfaces (APIs) and provide configurable data interfaces, such as programmable data items (PDIs). These APIs enable the development of software compatible with IAWSN for sensor nodes.

The IAWSN architecture is structured so that the data manager function and its corresponding software are application-agnostic. The configurable data interfaces ensure that customizing data exchange definitions for different applications does not necessitate software changes in the network manager; instead, defining and loading the PDI onto the network elements is sufficient. Data communication between network elements, as determined by the PDI, is managed by a data manager application running in the network manager. Thus, the combination of APIs, PDIs, and the data manager facilitates a seamless integration of sensor applications with the IAWSN, minimizing both effort and cost. The functional relationship among the APIs, PDIs, and data manager within the IAWSN is illustrated in Figure 3.9.

3.6.1 Performance Matrix

Developing new WSNs presents design challenges in meeting performance metrics related to network throughput, system latency, reliability, and network security. These performance metrics are influenced by the network's traffic

characteristics, which vary due to different data types and data rates required for operational needs at various phases-of-flight. The performance metrics typically include - fault tolerance, average system response, and waiting time.

Fault tolerance is explained in this chapter. In Chapter 4, a mathematical model for analyzing network traffic in a typical aircraft flight profile is presented. This model addresses different priority levels of multi-typed and multi-rated sensor data within an avionics network. The handling of priorities will be defined through mathematical expressions to evaluate network performance concerning system response for both low-priority and high-priority data. The models will be used to assess the QoS parameters of the network, specifically - average system response and waiting time.

Chapter 4 will also introduce a network simulation platform to evaluate the feasibility of MAC protocol selection for various scenarios in wireless avionics communications. Chapter 6 discusses a comprehensive security framework and network security analysis concerning threat profiles.

3.7 Chapter Summary

In this chapter, we have presented a fault-tolerant network architecture for IAWSN alongside the associated design challenges. We have proposed that Wireless Sensor Networks (WSNs) serve as a superior alternative to existing wired networks on aircraft. Our research work includes an approach for designing a robust, secure, adaptable, and scalable WSN while addressing the related design challenges. We have detailed the process of selecting the appropriate WSN architecture through a trade study. We have also described the design features of a representative WSN architecture in relation to key design drivers and performance requirements. Furthermore, we have presented a method for integrating various sensor-based applications with the proposed robust WSN while minimizing costs and time overheads.

Chapter 4

Throughput Analysis of WSN

4.1 Introduction

The new Intra Aircraft Wireless Sensor Network (IAWSN) is set to replace traditional wire harnesses within aircraft while maintaining or enhancing performance parameters. The key design drivers for the IAWSN include scalability, adaptability, and reliability. One promising application for the IAWSN is the Integrated Aircraft Health Management (IAHM) system, which will involve the installation of thousands of sensors on board the aircraft. Effective communication among various avionics components, actuators, and sensors—represented as network nodes or sensor clusters, will be crucial for the success of the IAHM system. The characteristics of these network nodes, particularly the sensors, are influenced by variations in data types, data rates, and data priority at different phases of flight. These factors will significantly affect the network's throughput and data loss performance in dynamic and safety-critical applications. Therefore, the network must be designed to effectively manage the Quality of Service (QoS) parameters.

The development of a high-performing network involves various design issues that include (i) choice of network topologies, (ii) allocation of frequencies for wireless nodes, and (iii) ensuring throughput, latency, reliability requirements of the network. Since these performance metrics are affected by traffic characteristics, a mathematical model tailored for network traffic analysis specific to the proposed Wireless Sensor Network (WSN) has been introduced. The model employs priority queuing theory to manage different priority levels of variable data types and variable data rates of sensor data within an avionics network. Preemptive and non-preemptive priority handling policies are utilized to formulate mathematical expressions for network traffic. These policies allow for a comparative analysis of network performance, particularly focusing on how the system responds to low-priority data in the presence of high-priority data. The model is applied to a representative network comprising six sensors, each with different priority levels and variable data rates, to evaluate key

QoS parameters, specifically: (i) average system response and (ii) waiting time. The network simulation platform described in this chapter serves as a tool for assessing the feasibility of different medium access control (MAC) protocol selections for various scenarios in wireless avionics communications.

This chapter presents a priority queuing model that addresses traffic dynamics during various stages of flight operations. The model operates independently of any specific protocol definitions. The aim is to analyze the variations in data traffic throughout each operational phase of an aircraft, including parking, taxiing, takeoff, cruising, approach, landing, and touchdown. Additionally, the model considers priority variations among different classes of sensors during these flight phases, alongside the dynamic characteristics of the data. A priority queuing model has been developed to evaluate the performance of a (WSN) with probabilistic traffic characteristics. This approach is beneficial as priority queuing simplifies computation and allows for stochastic network traffic analysis while accounting for priority variations. In the context of aircraft wireless network modeling, it is essential to manage the prioritization of sensors throughout the different phases of flight.

We also provide a general introduction to priority queuing policies that are currently in use, as well as the traffic model that includes specifications such as data frequency and priority across different flight phases. Our simulation results for the traffic model include representative data illustrating variations in priority, arrival intensities, and mean service times for different sensor classes. We assess performance parameters to characterize the network model effectively. The simulation results highlight the variations in QoS across different priority classes. Additionally, we discuss comparative studies of simulated throughput for prioritized versus non-prioritized data traffic [11].

4.2 Priority Queuing Model

A basic queuing model has been developed to analyze the traffic characteristics QoS of a WSN in an aircraft environment, where data rates and information priorities vary. In this model, data packets flowing through the network are referred to as customers, while the computing nodes are considered servers. Queuing theory provides a framework for the stochastic analysis of networks with probabilistic data traffic [95]. The primary goal of investigations in queuing theory is to determine the main performance measures of the system, which include the probabilistic characteristics (such as distribution function, density function, mean, and variance) of several random variables: the number of customers in the system, the number of waiting customers, the utilization of the servers, the response time of a server, waiting time of a customer, idle time of the server, and busy time of the server. Network performance is influenced by the distribution of inter-arrival times, service times, the number of servers, capacity, and service discipline. The above-mentioned system is assumed to follow a Markovian process to compute the distributions of these performance parameters.

For the sake of simplicity let us consider first a single-server system. Let ρ be called the traffic intensity, defined as:

$$\rho = \text{mean service time} \times \text{mean inter-arrival time} \tag{4.1}$$

Assuming an infinity population system with arrival intensity λ, which is reciprocal of the mean inter-arrival time, and let the mean service denote by $\frac{1}{\mu}$, then we have:

$$\rho = \text{mean service time} \times \text{mean inter-arrival time} = \frac{\lambda}{\mu} \tag{4.2}$$

Among the wide range of performance measures that we have for a queue model of a network, the ones which are significant in this context are the waiting and response times denoted respectively by W and T. The expected values are for system response and waiting time are defined as follows:

$$E[T] = \frac{1}{(\mu - \lambda)} \tag{4.3}$$

$$E[W] = \rho E[T] \tag{4.4}$$

Since, queueing analysis is all about finding out the distributions for QoS parameters, we are interested in the mean and variance of the performance measurement. Using Little's theorem we can also obtain a measure of average total number of customers N in the system and the number Q waiting to be served, as follows:

$$E[N] = \lambda E[T] \tag{4.5}$$

$$E[Q] = \lambda E[W] \tag{4.6}$$

With the background knowledge that we have as of now about the essential QoS parameters that qualify for the characteristics of the network concerning data traffic, we now introduce priority queues. Let us consider an $M/M/1$ system with priorities. This means that we have two classes of customers. Each type of request arrives according to a Poisson process with parameters λ_1, and λ_2, respectively, and the processes are supposed to be independent of each other. The service times for each class are assumed to be exponentially distributed with parameter $\frac{1}{\mu}$.

The system is stable if:

$$\rho_1 + \rho_2 < 1 \tag{4.7}$$

Where ρ_i has got its usual meaning and definition as stated earlier, with $i = 1, 2$.

Let us assume that class 1 has priority over class 2. The preemptive and non-preemptive systems may be used to calculate some mean values for the performance parameters described before.

4.2.1 Preemptive Policy

In a preemptive policy, the service for a customer in class 2 is never performed if there is a customer from class 1 in the system. This means that class 1 takes priority over class 2; if a class 2 customer is being served when a class 1 request arrives, the service for the class 2 customer is interrupted, and the service for the class 1 request begins immediately. The interrupted service for class 2 will only resume if there are no class 1 customers in the system.

If we classify the number of customers in the system into two categories—$N1$ for class 1 and $N2$ for class 2—then the average system response can be defined as follows:

$$E[T1] = \frac{\frac{1}{\mu}}{(1-\rho_1)} \tag{4.8}$$

$$E[N1] = \frac{\rho_1}{(1-\rho_1)} \tag{4.9}$$

$$E[T2] = \frac{E[N2]}{\lambda_2} \tag{4.10}$$

$$E[N2] = \rho_2/((1-\rho_1)(1-\rho_1-\rho_2)) \tag{4.11}$$

4.2.2 Non-Preemptive Policy

In a non-preemptive policy, the arrival of a class 1 customer does not interrupt the service of a class 2 request. This discipline is sometimes referred to as Head-of-Line (HOL) scheduling. In this situation, service for class 1 starts only after class 2 has been completed. By applying the law of total expectations, we can derive the mean response time for class 1.

$$E[T1] = \frac{E[N1]}{\mu} + \frac{1}{\mu} + \frac{\rho_2}{\mu} \tag{4.12}$$

By applying Little's theorem, we have:

$$E[N1] = \lambda_1 E[T1] \tag{4.13}$$

After substitution, we get:

$$E[T1] = (1+\rho_2)/(\mu(1-\rho_1)) \tag{4.14}$$

$$E[N1] = ((1+\rho_2)\rho_1)/(1-\rho_1) \tag{4.15}$$

Coming to the mean values for T_2 and N_2 we have as follows:

$$E[N2] = ((1-\rho_1(1-\rho_1-\rho_2))\rho_2)/((1-\rho_1)(1-\rho_1-\rho_2)) \tag{4.16}$$

By application of Little's law we have

$$E[T2] = \frac{E[N2]}{\lambda_2} = ((1 - \rho_1(1 - \rho_1 - \rho_2))\rho_2)/(\mu(1 - \rho_1)(1 - \rho_1 - \rho_2)) \tag{4.17}$$

4.3 Simulation Model for Aircraft WSN

The sensor network involved in flight operations is modeled using priority-based queuing theory. In this analysis, an $M/M/1$ queuing system is used, with dedicated servers for each category of sensor data transmitted over the network. Multiple servers are considered to represent the aircraft scenario, where various sensor applications process data from different sensor nodes. In this context, M refers to a Markovian process that follows a Poisson distribution for data arrivals. The model assumes infinite capacity, meaning that the arrival rate of data is independent of the number of customers being served. However, the servers have a finite queue length due to the limitations of available data bandwidth. The queue is limited by the maximum number of customers that can be processed in one unit of time, specifically 1 second. For modeling purposes, typical phases of flight operations—ranging from parking and taxiing to touchdown—are examined, and traffic intensity is analyzed for each identified phase of operation.

Network data traffic is characteristic of each phase and priority is subject to the duration of each operational stage. Table 4.1 illustrates the individual phases along with priority categories of sensor data. It shows the phase-wise distribution of associated sensor data rates (customers) and mean server processing rates for high and low-priority classes. Table 4.2 shows data classes numbered in Roman numerals which represent the particular type of state information being observed. The mean sensor frequencies and mean service times are also given along with each individual sensor class.

In this model, the arrival intensity of network data is computed considering the native sensor data rate as well as the rate of information flow. The reason is that, as part of network analytics, we are also concerned with the traffic of significant data that has information associated with it. Again information may not always be effectively represented by such continuous polling of high data-rate sensors. Not all state variables would be varying with such a high gradient at all instants. So the arrival intensity is defined as a weighted frequency of incoming data. The weight is further defined as the ratio of a particular operation phase duration to the total time of flight. This ensures an equitable distribution of the packet arrivals from the two classes of sensors during each operational phase. The assumption for the wireless network model is also true for wired networks. Following is an example of computation for a specific time sample with a duration of 1 second. In order to model effective arrival intensity over a duration of 1 second, the following simple heuristic is used.

Phase	Frequency (High Priority) [Hz]	Frequency (Low Priority) [Hz]	Server Rate (High Priority) [Hz]	Server Rate (Low Priority) [Hz]
Parking VI, V → High I, II, III, IV → Low	80	600	20	80
Taxi VI, V → High I, II, III, IV → Low	80	600	20	80
Takeoff I, II, III, IV, V → High VI → Low	600	80	80	20
Climb I, II, III, IV, V → High VI → Low	600	80	80	20
Cruise I, II, III, IV, V → High VI → Low	600	80	80	20
Approach I, II, III, IV, V → High VI → Low	600	80	80	20
Touch Down II, IV, V → High I, III, VI → Low	400	600	80	80
Taxi V, VI → High I, II, III, IV → Low	80	600	20	80
Parking V, VI → High I, II, III, IV → Low	80	600	20	80

Table 4.1: Flight Phase, Sensor Data Rates, Server Processing Rates

Class	Individual Sensors		
	Sensor Type	Frequency	Mean Service Time
I	Airspeed (AHM)	600 Hz	80 Hz
II	Attitude and Heading	400 Hz	80 Hz
III	Altitude (AHM)	100 Hz	80 Hz
IV	Engine Sensors (EHM)	80 Hz	40 Hz
V	Ground Speed (AHM)	80 Hz	20 Hz
VI	Proximity Sensors	10 Hz	10 Hz

Table 4.2: Sensor Data Class

Phase	**Arrival Intensity (High Priority)**	**Arrival Intensity (Low Priority)**	**Mean Service Time (High Priority) (secs)**	**Mean Service Time (Low Priority) (secs)**
Parking VI, V → High I, II, III, IV → Low	2	11	$\frac{1}{20}$	$\frac{1}{80}$
Taxi VI, V → High I, II, III, IV → Low	8	63	$\frac{1}{20}$	$\frac{1}{80}$
Takeoff I, II, III, IV, V → High VI → Low	6	4	$\frac{1}{80}$	$\frac{1}{20}$
Climb I, II, III, IV, V → High VI → Low	31	4	$\frac{1}{80}$	$\frac{1}{20}$
Cruise I, II, III, IV, V → High VI → Low	50	13	$\frac{1}{80}$	$\frac{1}{20}$
Approach I, II, III, IV, V → High VI → Low	31	4	$\frac{1}{80}$	$\frac{1}{20}$
Touch Down II, IV, V → High I, III, VI → Low	6	4	$\frac{1}{80}$	$\frac{1}{80}$
Taxi V, VI → High I, II, III, IV → Low	8	63	$\frac{1}{20}$	$\frac{1}{80}$
Parking V, VI → High I, II, III, IV → Low	2	11	$\frac{1}{20}$	$\frac{1}{80}$

Table 4.3: Arrival Intensity and Mean Service Times for Different Flight Phases

$$\lambda = (\frac{\tau_i}{\sum \tau_i}) \times f_{sensor} \tag{4.18}$$

Where,

- $\lambda \Rightarrow$ arrival intensity of customers
- $\tau_i \Rightarrow$ duration of each phase of flight
- $\sum \tau_i \Rightarrow$ total duration of flight
- $f_{sensor} \Rightarrow$ operational frequency of the sensor

Table 4.3 accordingly presents arrival intensities and mean service times for every individual phase of the flight operation:

4.4 Results and Analysis

Mean service times and arrival intensities, computed from equations 4.15-4.18, are sufficient parameters within the context of the priority queue model. This

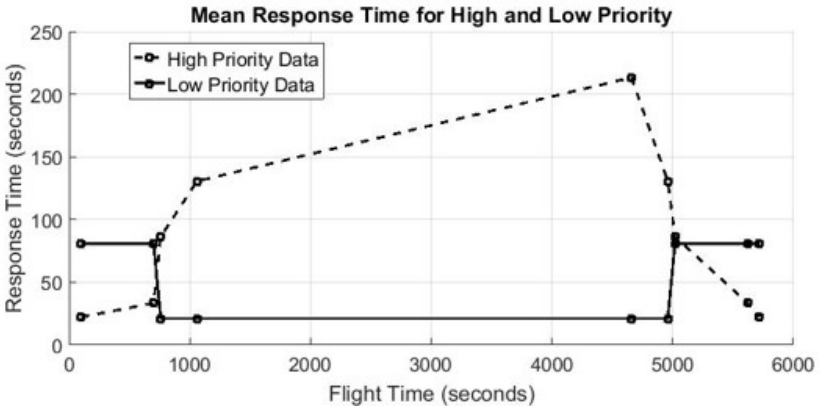


Figure 4.1: Average System Response for High and Low Priority Data Traffic Simulated Using General M/M/1 Queuing Model

model, proposed for analyzing traffic within the network of end-systems in an aircraft, has been tested through simulations for both preemptive and non-preemptive queueing analysis.

In the traffic analysis of the proposed wireless aircraft sensor network, priority queuing and general queuing models are compared. Key QoS parameters include average system response time, the number of customers in the system, and waiting time in the queue.

Figure 4.1 illustrates the phase-wise variations of high and low data traffic in the WSN over a typical flight duration. A $M/M/1$ queuing model is used to analyze the average system response for prioritized data. It can be observed that high-priority data suffers from low response times because the model considers only the traffic intensity of incoming data, regardless of priority, during the respective phases. During the phases from climbing to descent, high arrival intensity exists for high-priority data traffic, resulting in an increased average system response time.

Figure 4.2 shows the variations in the average waiting time for high-priority data during the climbing to descent phases. This is consistent with the variations in system response depicted in Figure 4.1. It is evident from Figure 4.2 that the throughput of high-priority data traffic is compromised during the mid-course flight phases.

Suitable policies need to be adopted to maintain better throughput for high-priority data consistently. As discussed in the earlier section on an introduction to queueing theory, preemptive queueing tends to reduce the system response time for low-priority data. As shown in Figure 4.3, the simulated response times for low-priority data increase significantly during the climb, cruise, and approach phases, registering -0.2, 0.5, and 0.2 seconds respectively. This is primarily due to the increased data arrival intensities of high-priority data during these phases. Low-priority data is preempted more frequently because of the

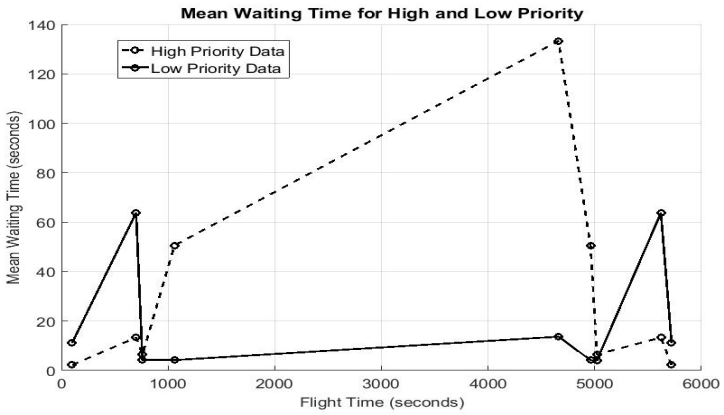


Figure 4.2: Average Waiting Time for High and Low Priority Data Traffic Simulated Using General M/M/1 Queuing Model

high traffic density of high-priority data. The low system response to low-priority data under the preemptive scheme during the main flight phases is consistent with other QoS parameters that have been simulated. The average system response for low-priority data during the climb, cruise, and approach phases improves under a non-preemptive policy, as shown in Figure 4.4. However, the system response for high-priority data in the taxi and touchdown phases is poorer due to low mean service rates. Therefore, the non-preemptive approach compromises priority in favor of mean service time. Additionally, the low utilization of the high-priority server in most phases is supported by the average number of customers N, as shown in Figures 4.5 and 4.7. The mean values of N differ for preemptive and non-preemptive policies, with N being lower in most phases compared to the processing capacity of the servers.

However, priority queuing improves the throughput of high-priority data as is evident from Figures. 4.6 and 4.8, where high-priority data traffic faces lesser waiting time than what is achieved in general queuing-based characterization. CSMA-based MAC protocols can be implemented to improve the low utilization of the high-capacity servers particularly during the parking and taxi phases. On the other hand, TDMA-based access protocols can be allowed for the rest of the phases, wherein the data packets from the low-priority class can be given an equitable share of network access. This is because the queueing model, as presented here considers only the traffic intensities of data flowing in the network. Contention of data transmission by the nodes and collision has not been considered in the present model. The model can be used even when we resort to TDMA for some networks. Coming back to the results, average N during the climb, cruise, and approach phases is greater in preemptive policy (Figure 4.3), in comparison to the non-preemptive (Figure 4.5), while traffic intensity is higher for the low priority class during the three phases.

As a result, average system response time increases for the low-priority ones.

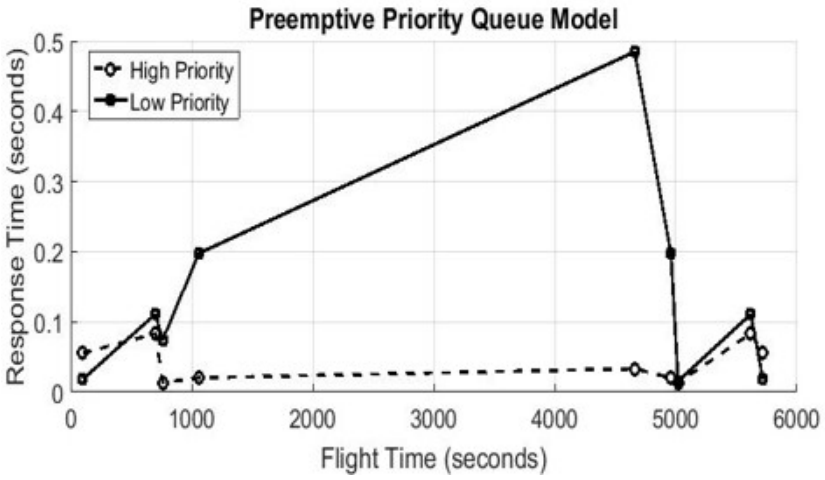


Figure 4.3: The preemptive queueing simulations showing system response time for both high as well as low priority based data classes. The X-axis is the total duration of a typical flight consisting of phases as enlisted in Table 4.1

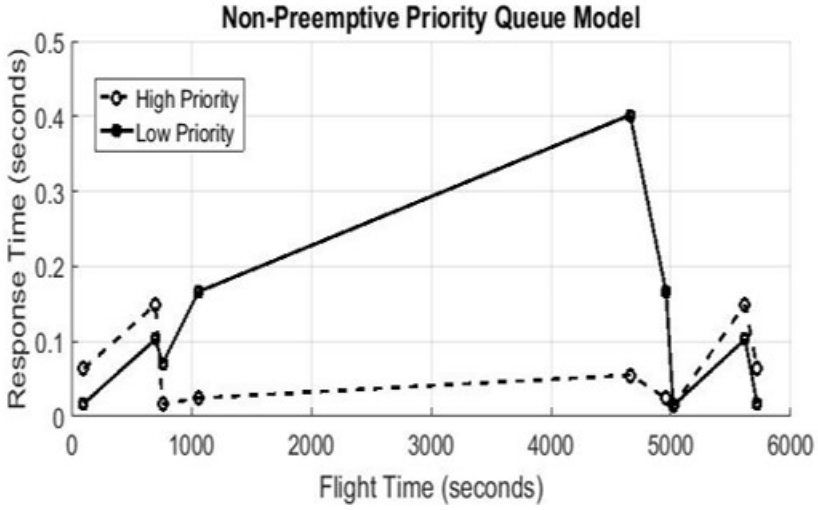


Figure 4.4: The non-preemptive queueing simulations showing system response time for both high as well as low priority based data classes. The X axis is the total duration of a typical flight consisting of phases as enlisted in Table 4.1

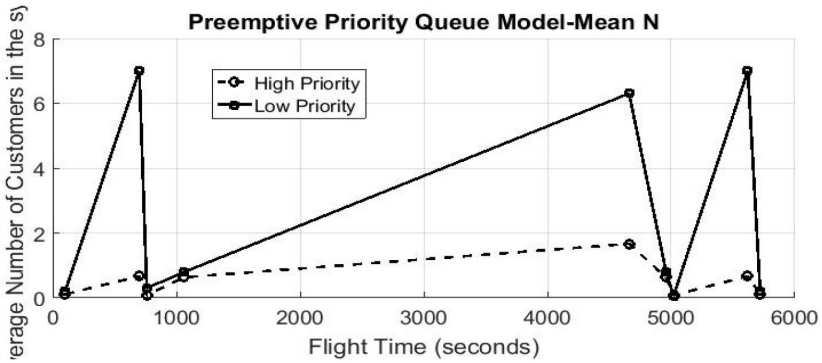


Figure 4.5: The preemptive queueing simulations showing average number of customers in the system for both high and low priority data classes. The X axis is the total duration of a typical flight consisting of phases as enlisted in Table 4.1

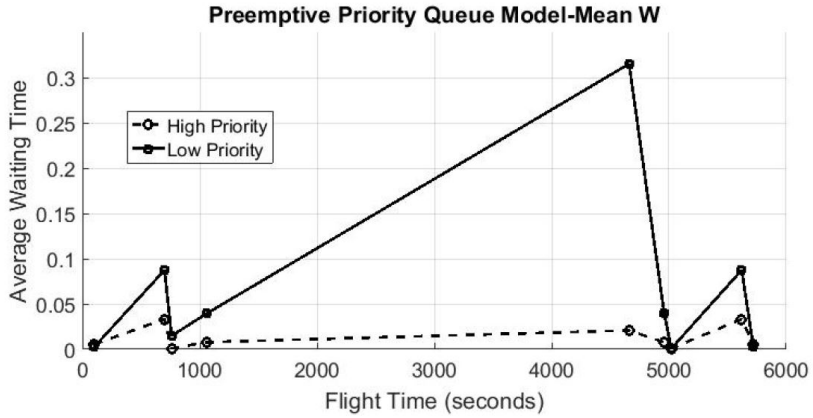


Figure 4.6: The preemptive queueing simulations showing average waiting time for customers in the system for both high and low priority data classes. The X axis is the total duration of a typical flight consisting of phases as enlisted in Table 4.1

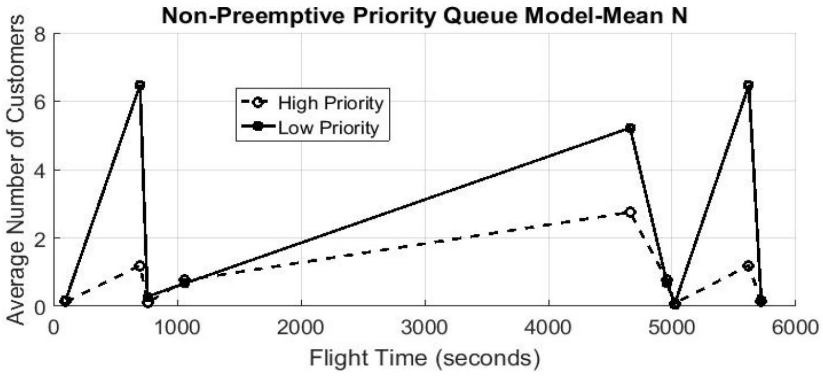


Figure 4.7: The non-preemptive queueing simulations showing average number of customers in the system for both high and low-priority data classes. The X axis is the total duration of a typical flight consisting of phases as enlisted in Table 4.1.

QoS	General Queuing		Priority Non Preemptive Queuing		Priority Preemptive Queuing	
	High	Low	High	Low	High	Low
Maximum System Response (seconds)	210	80	0.18	0.4	0.1	0.5
Maximum Waiting Time (seconds)	130	65	0.25	6.5	0.04	0.3

Table 4.4: Comparative QoS for Different Queuing Models

It is evident from Table 4.3 that during the parking and taxi phases, the mean service time for the low-priority class is higher than the high-priority one. This again results in low traffic intensity, and thus, response time is lowered even for low-priority data compared to the other class. As a result, the server for low-priority data during these phases remains mostly unutilized. Table 4.4 presents a comparative summary of the QoS predictions obtained by using general and priority queuing models (with pre-emptive and non-preemptive policies). The general queuing model is ineffective in analyzing traffic characteristics for prioritized data.

The preemptive policy is more effective in improving the average system response for low and high-priority data, with reduced waiting time for both priority classes compared to non-preemptive priority queuing.

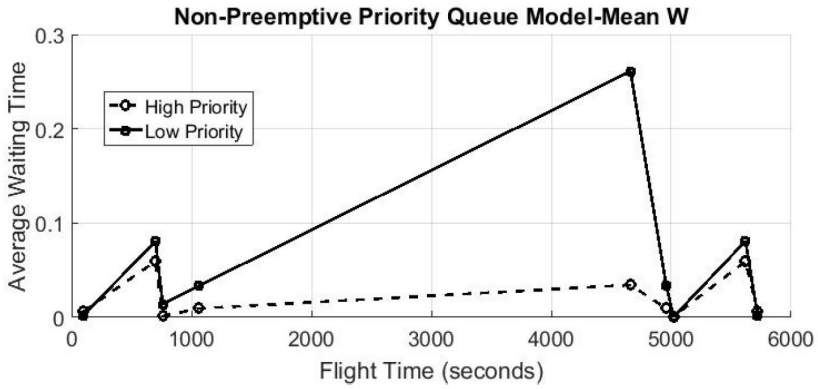


Figure 4.8: The non-preemptive queueing simulations showing average waiting time for customers in the system for both high and low priority data classes

4.5 Chapter Summary

This research focuses on developing and studying a priority queueing model that considers variations in the priority of sensor data during different phases of flight operations. Based on network requirements, a priority-based queueing model has been implemented, and traffic distributions concerning the frequency of data transmitted by various sensors into the communication network at different flight phases are analyzed.

Both preemptive and non-preemptive policies are employed to develop the model for stochastic analysis of the various QoS parameters relevant to assessing the network's response to dynamic traffic characteristics. It has been observed that the non-preemptive policy is more effective than the preemptive policy for averaging the system response to data flow in a typical intra-aircraft WSN. Additionally, traffic characterization using priority queueing policies has proven to be superior to that achieved with general queueing models.

The experiments conducted are effective in determining the appropriate MAC protocol, facilitating the development of a wireless sensor network that meets specified requirements.

Chapter 5

CDMA Based Approach For QoS Improvement

5.1 Introduction

In the previous chapters we have analyzed the multi-layered architecture and priority queuing model to implement Intra Aircraft Wireless Sensor Networks (IAWSNs). Throughout our research, we have recognized the importance of ensuring robust and reliable communication for applications such as Intra-Aircraft Health Management (IAHM), Structural Health Monitoring (SHM), and autonomous systems for next-generation aviation. Additionally, we discussed that IAWSNs must be designed for reliable performance under various operational conditions and must coexist with other wireless systems, like Wi-Fi and Bluetooth, which often operate within the same environment. We have determined that the IEEE 802.15.4 protocol is an excellent choice for low-power and low-data-rate communication, making it well-suited for wireless sensor networks. Its energy efficiency supports battery-powered sensor nodes, which is critical for many applications. However, the protocol's limited data rate may become a bottleneck when addressing the advanced connectivity needs of modern aircraft.

Several challenges have been identified in deploying IEEE 802.15.4-based IAWSNs, particularly for large-scale applications such as SHM and IAHM. These networks face significant interference from Wi-Fi and Bluetooth devices, and electromagnetic noise from other onboard systems. The shared use of the 2.4 GHz ISM frequency band further complicates these challenges, impacting key Quality of Service (QoS) parameters such as throughput, latency, and Packet Error Rate (PER).

To address these challenges, we have explored the potential of integrating Code Division Multiple Access (CDMA) with IEEE 802.15.4. CDMA has been proven effective in cellular networks as a reliable solution for interference-free communication, particularly in large-scale deployments. Following are some

of the key benefits by applying CDMA to IAWSNs:

1. **Enhanced Interference Mitigation:** CDMA effectively minimizes interference from coexisting networks by allowing multiple devices to transmit simultaneously over the same frequency band using unique codes.
2. **Improved Signal-to-Noise Ratio (SNR):** CDMA's ability to spread signals across a wide frequency band enhances resistance to noise and interference, leading to more reliable communication.
3. **Better Throughput and Scalability:** CDMA enables IAWSNs to support a higher number of sensor nodes without significantly degrading performance, addressing scalability concerns for large-scale applications.
4. **Reduced Packet Error Rates (PER):** By mitigating interference and improving signal clarity, CDMA helps lower PER, ensuring more consistent data transmission.
5. **Increased Flexibility in Frequency Sharing:** CDMA allows IAWSNs to coexist more harmoniously with other wireless technologies operating in the ISM band.

We have proposed and simulated a CDMA-based communication scheme tailored for IAWSNs operating under IEEE 802.15.4. Through simulations, we have evaluated its performance against the standard protocol in scenarios involving interference from both IAWSN nodes and Wi-Fi devices. The results have demonstrated clear improvements in QoS metrics such as SNR, Bit Error Rate (BER), operational bandwidth, and Process Gain. We have identified specific design changes required for legacy IEEE 802.15.4 transceivers to make this integration feasible. These modifications pave the way for enhanced performance and a more robust IAWSN framework. The insights gained from this study also highlight areas for further research, opening new possibilities for advancing IAWSN technology.

5.2 Spread Spectrum Communication and CDMA Technology

CDMA is a multiple access technique used in cellular networks to allow multiple users to share the same frequency band simultaneously. Each user is assigned a unique code that is used to modulate their signals, and these codes are orthogonal to each other, which allows multiple users to transmit at the same time without interfering with each other. CDMA is widely used in 2G, 3G, and 4G cellular networks.

CDMA uses direct sequence spread spectrum (DSSS) technique which takes the digitized version of an analog signal and spreads it out over a wider bandwidth at a lower power level. The digitized signal in serial data form is spread

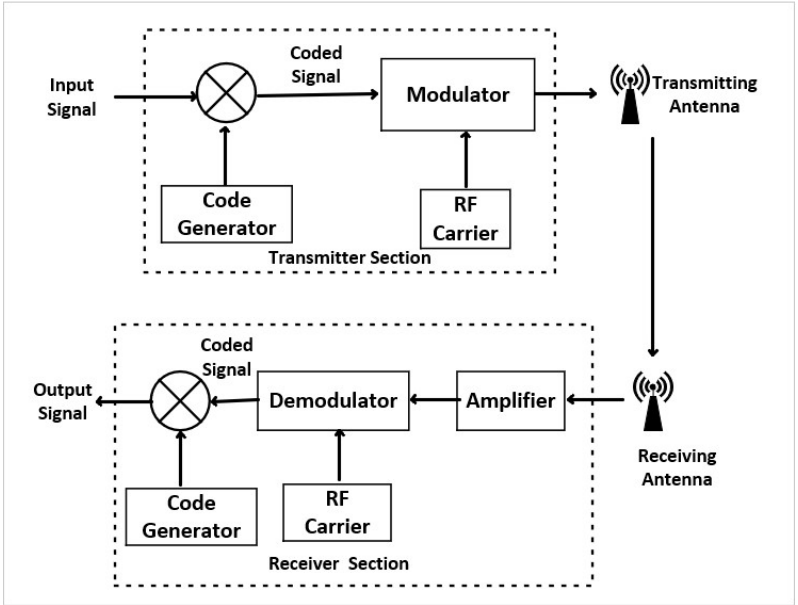


Figure 5.1: CDMA Communication System

by processing it in an XOR circuit along with a chipping signal at a much higher frequency (Figure 5.1). The chipping signal is derived from a pseudo-random code generator that assigns a unique code to each user of the channel. This code spreads the signal over a much larger bandwidth compared to the original. The resulting signal is at a low power level and appears more like noise. Many such signals can occupy the same channel simultaneously. For example, using 64 unique chipping codes allows up to 64 users to occupy the same channel at the same time. At the receiver, a correlating circuit finds and identifies a specific transmitter's code and recovers it [96].

5.3 Challenges in IAWSN Design for Large Scale Networks

One of the most promising application areas of IAWSN is aircraft structural and system health monitoring. Health monitoring applications like SHM, PHM, EHM, etc. require large number of sensor nodes with the option of further scalability.

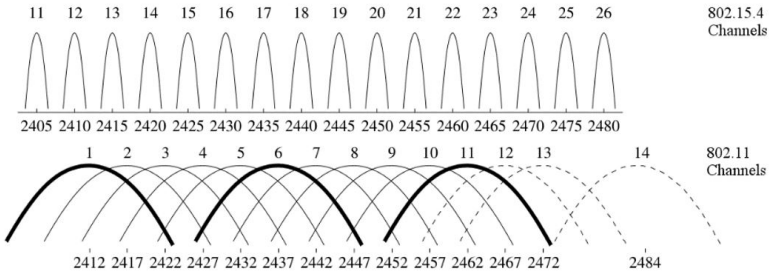


Figure 5.2: Channel Spectra of 802.15.4 and 802.11

5.3.1 Spectrum Sharing and Co-Existence Problem

Well-accepted wireless communication technologies generally operate in frequency bands that are shared among several users, often using different RF schemes. This is true in particular for IEEE 802.11, Bluetooth LE, and IEEE 802.15.4 protocols. They operate in the unlicensed 2.4 GHz band, also known as ISM band, which has been key to the development of a competitive and innovative market for wireless embedded devices. But, as with any resource held in common, it is crucial that those technologies coexist peacefully to allow each user of the band to fulfill its communication goals. Despite efforts made by standardization bodies to ensure smooth coexistence it may occur that communication technologies transmitting for instance at very different power levels interfere with each other.

Wireless technologies such as IEEE 802.11 (WiFi) and IEEE 802.15.4 often operate in the same frequency range, which can lead to cross-technology interference (CTI) between the signals of the two protocols, affecting the performance of both [97]. In particular, it has been pointed out that IEEE 802.15.4 could potentially experience interference from WiFi traffic since WiFi transmissions usually occur at much higher power level [97]. Figure 5.2 shows the overlapping of the channels of IEEE 802.15.4 and WiFi which is the primary cause of interference. IAWSNs, when deployed, must co-exist with other wireless devices and networks based on WiFi and Bluetooth technologies. Sharing of the ISM frequency band (2.4 GHz) among these networks makes the co-existence problem more challenging and has a significant impact on the Quality of Service (QoS) in terms of throughput, latency and Packet Error Rate (PER) of WSN. There are various channel management, priority-based scheduling and time-sharing techniques that are deployed currently to address the co-existence problem. However, these methods perform a trade-off among one or more operational parameters like channel bandwidth, number of nodes per channel, throughput, latency, PER, etc. of WSN.

5.3.2 Design Challenges

The IEEE 802.15.4 has been designed for low power low data rate communication. While low power is a desirable feature for sensor networks and enable battery powered sensor node operations, low data rate may not always be a desirable / sufficient feature especially for certain aircraft system health monitoring applications where the sensor sampling and update rates are higher for example vibration measurements. WiFi could be an alternative from the data rate perspective but the power consumption of WiFi devices due to high transmit power are not suitable for large scale sensor networks on aircraft. Though IEEE 802.15.4 offers 16 channels for data communication, the usable bandwidth per channel is 2 MHz which translates to a gross maximum data rate of 256kbps. Considering the protocol overheads, the effective achievable rate for the useful data is less than 200 kbps on an average. The underlying mechanism for media access in IEEE 802.15.4 communication is CSMA-CA which works better for small scale operations with reasonable reliability.

However, as the scale of the network increases, the data latency and packet loss increase especially on single channel operations due to long waiting time for media access, collisions, and resultant re-transmissions. Thus, the overall communication reliability comes down drastically in large scale networks. One of the possible methods for overcoming the above problem is to use a combination of channel switching with CSMA-CA. However, this introduces additional complexity in the implementation and might lead to additional delays due to frequent channel switching. IEEE 802.15.4 also provides the option of Time Division Multiple Access (TDMA) which improves reliability by avoiding the need for waiting time to access the channels and also minimizes the collision and packet loss compared to CSMA-CA. As the number of nodes operating on a given channel increases, allocating time slots for more number of relatively high data rate or high priority nodes becomes a challenge and will lead to more interference and packet loss. This can be mitigated to certain extent by allocating distinct channels for each cluster of nodes and allowing each cluster to manage its own TDMA. However, the maximum throuhgput per channel (< 200 kbps) still remains as a limitation. The problem of narrowband interference due to Wi-Fi, Bluetooth and other IEEE 802.15.4 device is reduced to some extent by the DSSS implementation in basic IEEE 802.15.4 standard. However, the maximum throughput per channel (128 kbps) remains as a limitation. Also, since the number of orthogonal chip sequence for DSSS is 16, if the number of nodes in a cluster is more than 16 then the inter nodal interference begins due to the use of the same chip sequence by multiple nodes. Hence, the design requirements for IEEE 802.15.4 based intra aircraft sensor networks have been formulated as follows:

- Retain the low power operation of the basic protocol.
- Increase the data rate to at least couple of Mbps levels to support wide range of use cases.

- Support large scale network operations with acceptable QoS i.e packet/bit error rate and latency.
- Should be capable of operating simultaneously with Wi-Fi networks with minimal or no impact on QoS i.e packet/bit error rate and latency. A CDMA based PHY layer is proposed for 802.15.4 radio to achieve the above requirements of an IAWSN.

5.4 Implementation of CDMA in IAWSN

A CDMA based schema is implemented for a representative use case and is analyzed for its performance against the design requirements defined for the 802.15.4 based IAWSN in the previous section. Implementation of this schema and also other features dictated by the design requirements of IAWSN demands changes in the PHY and MAC layers of the 802.15.4 radio. This chapter is focused primarily on the PHY layer changes. MAC layer changes could be taken up in future research. A comparative analysis of the performance of the proposed CDMA schema and the existing CSMA-CA of 802.15.4 protocol is performed to establish the advantages of the CDMA schema. Structural health monitoring (SHM) of the aircraft is chosen as the representative use case for this purpose.

5.4.1 IAWSN for Aircraft Structural Health Monitoring

A conceptual architecture of the SHM is shown in Figure 5.3. SHM for an aircraft involves monitoring of thermal and aerodynamic loads acting on various zones of the aircraft body. These loads are calculated by measuring the stress, temperature, and vibration with the help of sensors distributed all over the aircraft body. The proposed solution involves the introduction of wireless connectivity between these sensors, data managers and processors.

Out of all the parameters that are measured, vibration data requires the highest sampling rate due to its high frequency variation. The sampling rate may go up to 10 kHz depending on the nature of analysis to be performed and the expected outcome. Also, the level of precision required in the vibration data is more from the analysis point of view. Single precision floating point (16 bits) may not be sufficient for many applications, and hence double precision floating point (32 bits) will be required. Considering the worst-case scenario of 10 kHz sampling rate and the double precision, the throughput required for transferring a single parameter from a single sensor is 320 kbps. As we consider more parameters and more sensor nodes, the throughput requirement is likely to increase multifold to reach megabits per second (mbps) scale. For the purpose of modeling, an arbitrary throughput requirement of 2 Mbps is considered. Clearly, this is not achievable with the existing physical layer schema of 802.15.4 standard since its maximum throughput specification is only 256 kbps. As discussed before, after considering the bits allocated for

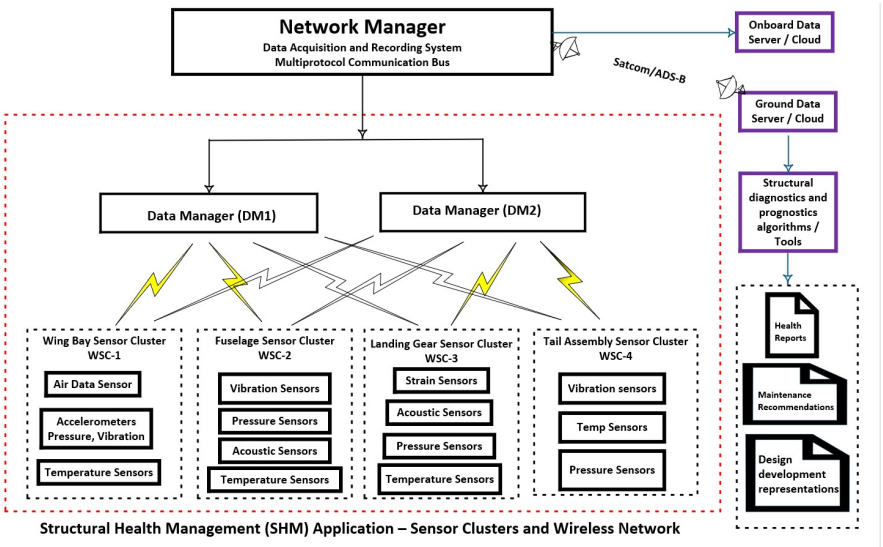


Figure 5.3: Aircraft Structural Health Monitoring System

protocol overheads, the useful data rate that is achievable practically is less than 200 kbps.

5.4.2 PHY Layer Changes in IEEE 802.15.4 Transceiver

There are various PHY layer variants available in 802.15.4 for 2.4 GHz operation. We have selected the commonly used PHY layer OQPSK PHY which also offers 256 kbps. The conceptual diagram of OQPSK schema is shown in Figure 2. Currently, OQPSK modulation is applied on one of the 16 channels used by a device. The total bandwidth available per channel is 2 MHz. The O-QPSK PHY employs a 16-ary quasi-orthogonal modulation technique. During each data symbol period, four information bits are used to select 1 of 16 nearly orthogonal pseudo-random noise (PN)sequences to be transmitted. The PN sequences for successive data symbols are concatenated, and the aggregate chip sequence is modulated onto the carrier using offset quadrature phase-shift keying (O-QPSK) to achieve a data rate of 256 kbps using 2MHz bandwidth.

In order to achieve higher data rate with the OQPSK schema, we need larger bandwidth. Also, The bandwidth required for achieving the data rate of 2 Mbps with OQPSK can be calculated from first principles of the schema as shown in the Table 5.1.

The current channel design for 802.15.4 specifies 16 channels of 5 MHz each (2 MHz useful band, 3 MHz guard and) hence a total bandwidth of 80 MHz. In order to achieve the increase data rate of 2 Mbps, we need a useful bandwidth of 32 MHz as shown in 5.1. Hence, the current channel segmentation of 802.15.4 has to be modified to achieve this. It is proposed to re-segment the total

Target Bit Rate	24 Mbps
Number of bits per symbol (in OQPSK)	4
Symbol Rate	2 Mbps / 4 = 0.5 Msymbols/s
Length of PN sequence (Walsh 64 code is proposed for CDMA implementation)	64
Chip Rate	64 chips/symbol
Bandwidth Required for achieving the symbol rate	0.5 MSymbols/s × 64 = 32 MHz

Table 5.1: Required Channel Bandwidth Calculation for Higher Data Rate

Total Bandwidth	80 MHz
Proposed No.of channels	2
Bandwidth per channel	40 MHz (32 MHz main band; 8 MHz guard band)

Table 5.2: IEEE 802.15.4 Channel Bandwidth Re-segmentation

bandwidth of 80 MHz as shown in Table 5.2. Commonly used ratio for guard band allocation is 10-25 percentage of the main band. 8 MHz guard band could be a reasonable choice in this context. However, further research can attempt to establish a method to determine the guard band considering the waveform schema, pulse shaping and the nature of side lobes in the practically achievable spectrum.

The next modification proposed in the PHY layer is the modification of the orthogonal PN sequence used for spreading the message bits. Currently, the 16 chip sequences of 32 chip length are purely used for achieving higher immunity against the narrowband noise by spreading the bandwidth. However, they do not provide a unique ID to the nodes as in the case of CDMA systems. Hence, the probability of correlation between the transmissions from multiple sensor

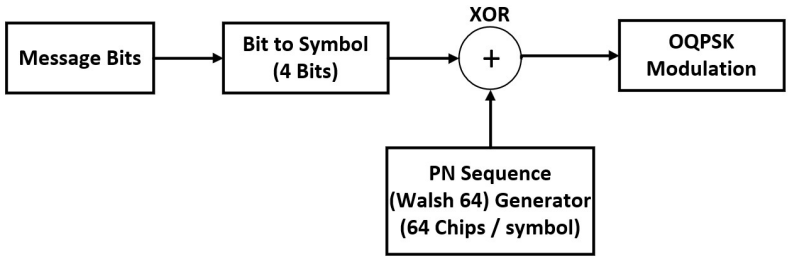


Figure 5.4: CDMA Modulation Schema for 802.15.4 PHY

nodes using the current schema is high whenever the message symbols sent by them match (each message symbol is mapped to one of the 16 chips in all the devices in the network). It is proposed to use a synchronous CDMA code 5.4 in place of the chip sequence through which every sensor node is assigned a unique code which serves as the unique identifier of the node as well as for spreading the spectrum. Number of such unique codes can be decided based on the number of nodes to be accommodated in a cluster. For example, 64 Walsh codes can be chosen for a cluster or a network of up to 64 nodes. If the number of nodes are more than the available codes, isolation can be achieved through spatial arrangement of the nodes in such a way that the transmissions from nodes using the same code do not interfere taking advantage of their communication range limit. However, the length of the code can be decided based on the amount of spread required. For the use case chosen for the modeling, the length of the Walsh 64 code sequence (64) is used. Since the CDMA code serves as the ID of a node, the short address field (16 bits) in the 802.15.4 protocol header becomes redundant and those bits could be used for increasing the data payload size.

5.5 Communication Performance and QoS Evaluation

Theoretically, the BER of a communication system is directly related to the SNR that can be achieved at the output of the receiver.

SNR = Received signal power (dB) – Noise power at receiver (dB)

Received signal power = Tx signal power (dB) + Tx antenna gain – channel path loss + Rx antenna gain

Receiver noise power = Thermal noise power (dB) + Interference noise (dB) + Noise figure (dB)

When comparing the standard IEEE 802.15.4 system with the proposed CDMA based system, the primary difference is the bandwidth of the modulated signal and the type of code used for spreading the signal that is transmitted while all other parameters are common. This can have the following effect on the parameters affecting the SNR and BER.

1. Increased thermal noise since it is directly proportional to the bandwidth.
2. Reduction in narrowband interference noise power due to the spreading of the interference noise with a highly orthogonal code while dispreading the received signal.
3. The interference noise reduction achieved is higher than the increase in thermal noise power thus reducing the overall noise power in CDMA system compared to the current system.
4. Reduced noise power leads to better SNR and BER.

Thus the proposed CDMA based system is expected to provide better QoS in terms of BER in presence of interference from other 802.15.4 devices using either the current standard design or the proposed CDMA design.

In order to validate the CDMA system against the above performance expectations, the following simulation experiments were conducted.

5.5.1 Performance Comparison under Co-Channel

Co-Node Interference: The co-node / co-channel interference in standard IEEE 802.15.4 communication has been studied extensively in the literature. Work presented in [98] deals with the hidden node collisions problem which are common in large scale and/or widely distributed 802.15.4 sensor networks. The IEEE 802.15.4 standard uses the blind back-off CSMA/CA channel access mechanism. The CSMA/CA channel access mechanism prevents collisions as long as all devices are in mutual radio range and can communicate directly with each other. Devices which cannot directly communicate with each other can start simultaneous transmission which will cause hidden node collision, despite use of the CSMA/CA. Hidden node problem is directly related to co-channel / co-node interference, where the interfering transmission is not strong enough for the performance for performing clear channel assessment by other nodes but are capable of causing interference and data errors in the reception of other nodes in the network.

Co-channel interference occurs when there are one or more interfering signals present in the same channel during communication between primary transmitter and receiver. During the packet reception, the receiver is synchronized with the transmitted signal and received chips are sampled for both I and Q phases. The interfering signal arrives at the receiver with time varying phase offset caused by initial phase offset and by frequency offset caused by the difference between the local oscillators in the receiver and in the source of the interfering signal [98].

After the O-QPSK demodulation, despreading is used to reduce the influence of chips errors. The received chip sequence will be decoded incorrectly as another PN sequence, if the number of chip errors is between packing radius and coverage radius of the PN sequence. Incorrect decoding of a PN sequence will lead to a symbol error and up to 4-bit error since each sequence is mapped to a symbol of length 4 bits [98].

The PN sequences used in the standard 802.15.4 implementations are not perfectly orthogonal. Also, each of them are mapped to one of the 16 symbols. Hence, the probability of correlation between the transmissions from the primary transmitter and other interfering transmitters is higher compared to the proposed CDMA implementation especially when the bit streams from two transmitters coincide partially or fully. On the other hand, the proposed CDMA based 802.15.4 system uses Walsh 64 code which has fully orthogonal set of 64 PN sequences and have been proven to be effective in the cellular network. Hence, it is expected to provide much superior performance compared to the current standard implementation especially when used for large

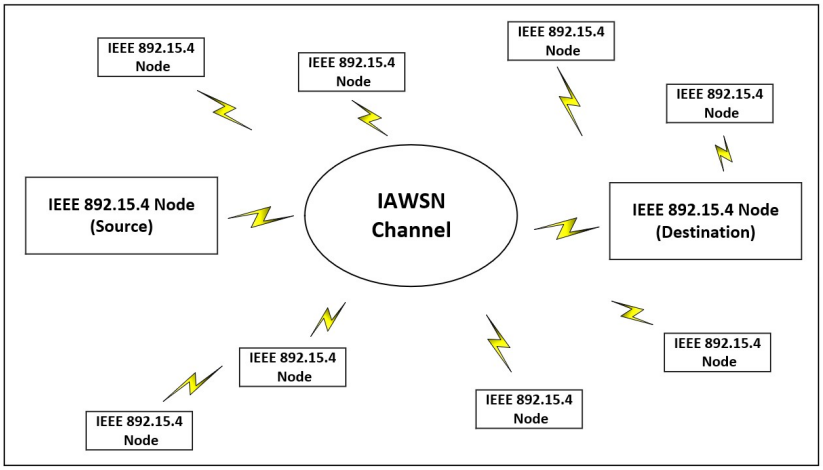


Figure 5.5: Network with Peer-Node Co-Channel Interference

scale networks. This system can support simultaneous transmissions from 64 nodes (each node assigned with one of the 64 orthogonal codes) without any interference at a much higher data rate utilizing the complete 32 MHz of useful channel bandwidth. However, the maximum nodes supported with full performance is theoretically restricted to 64 due to the maximum number of available orthogonal codes. Though, it is possible to duplicate the code assignments to two users when the number of nodes exceed 64, it leads to sub optimal performance due to the mutual interference between duplicated nodes. The experimental model for comparative study of the effect of increase in number of nodes on an IAWSN based on the standard implementation and the CDMA implementation is shown in Figure 5.5. Data transmission from source IEEE 802.15.4 node to another node is simulated in the presence of interference from other 802.15.4 nodes using the standard implementation first and the proposed CDMA based implementation subsequently. The distance of interfering nodes with respect to the receiving node are simulated as Poisson point process with a mean of 10 m (same as the distance between the primary transmitter and receiver nodes) to keep the interference diverse power-wise. The number of interfering nodes is gradually increased and the resultant changes in SNR and BER of the data transmission are recorded. The SNR and BER variations are plotted as a function of number of nodes for the standard 802.15.4 and CDMA implementations for comparative analysis.

5.6 Chapter Summary

In this research, we have analyzed the problem of co-existence of wireless communication systems onboard aircraft and addressed it by minimizing the interference between them. For QoS analysis we have studied the wireless

systems operating as per IEEE 802.15.4 and IEEE 802.11 (Wi-Fi) on the aircraft. We have narrowed down the problem to ensure minimization of interference due to the co-existence of IEEE 802.15.4 based communication devices and Wi-Fi network onboard aircraft.

1. We have developed a CDMA based communication scheme and simulated for a 802.15.4 based communication device with the objective of making it more immune to the high power interference from the Wi-Fi devices.

2. We have evaluated the communication performance of the CDMA based scheme by analyzing the QoS parameters like Bit-Error Rate, SNR and Eb/No for various combinations of Pseudo Random (PR) code generation algorithms and modulation methods through simulation. The performance analysis results show that the CDMA based design

3. We have brought out a significant improvement in the immunity of IEEE 802.15.4 network to Wi-Fi signal interference.

Choosing a right combination of the PR code generation algorithm and modulation technique is key to achieve the desired performance level for a specific system / application given its technical (processing power, memory, interfaces data rate, etc) and non-technical constraints.

Chapter 6

Security Framework for Intra-Aircraft WSN

6.1 Introduction

Efforts to replace wires with wireless network on board aircraft is increasing after the grant of Wireless Avionics Intra-Communication (WAIC) Band, a 200MHz spectrum (4.2GHz – 4.4GHz) exclusive band for inside aircraft communication by International Telecommunication Union (ITU) [6]. Drive to implement Integrated Aircraft Health Management (IAHM) in the next generation aircrafts and retrofit for in-service platforms calls for deployment of additional sensors in the order of tens of thousands and associated storage, computation and communication infrastructures. Aircraft being a safety critical system, it is important to ensure that manufacturers deploy a highly secure network inside aircraft and assure the safety levels as per safety and security standards of aircraft design, operation and maintenance.

Development of a robust and optimized security framework is the key for successful deployment of WSN scalable for WAIC. Need for wireless network onboard aircraft has already been established undisputed, efforts are now mobilized in industry to its advantage in all phases of aircraft life cycle - aircraft design, operation, maintenance, repair and overhaul. However, most of the exiting research present frameworks of secure wireless networks for industrial and process applications. Considering the opportunities and challenges of adopting the same to inside aircraft applications - we see a gap in maturity in implementation of security solutions for inside aircraft wireless network.

This chapter presents an optimized security architecture with group based key management scheme, a dynamic cryptography algorithm and a scheme for optimization of cryptographic algorithms that yields computational light weight modules capable of executing in resource constrained environment onboard aircraft. It also provides an empirical evaluation of the strength of network security by analyzing the resilience of connection between any two

sensor nodes for node capture and node compromise due to adversarial attacks. At the end, this chapter presents performance analysis of critical elements like: strength of the encryption keys and impact on network throughput due to computation and network overheads.

6.2 Security Architecture

The fundamental requirements of the wireless network discussed in the previous section are: (1) connecting avionics and related subsystems, (2) ensuring secure data transmissions for safety-critical operations, and (3) meeting latency requirements [10]. Since onboard aircraft systems have constraints on computational resources, there is a need for a lightweight security scheme. Therefore, this research focuses on the development of a security scheme that performs with optimal computational efficiency and has minimal impact on data streaming.

In this section, we consider a threat model that includes scenarios where data packets may be tampered with during transmission over a short-range wireless network inside an aircraft environment. Current FAA guidelines, regulations, and standards do not address these cybersecurity vulnerabilities.

The terms of reference document addresses cybersecurity concern and references the RTCA standards committees SC-236, SC-216, and EUROCAE WG-96 [99] [100]. The threat profiles considered in the proposed network include: breaching confidentiality by gaining unauthorized access to the network, eavesdropping, manipulation (man-in-the-middle attacks) that compromise network integrity, and network disruptions leading to Denial of Service (DoS) attacks.

An enterprise network is typically vulnerable to intrusions due to the presence of additional malicious computational sources, which can lead to the compromise of data confidentiality and integrity. In contrast, the present work assumes an adversarial mode of attack that can degrade network QoS in terms of throughput, BER, PDR, etc., and may even result in a breach of data security. To provide robust security for multiple sensor node clusters, it is crucial to manage cryptographic keys in an agile, coordinated, and organized manner. Therefore, a decentralized security architecture is considered in our research. The proposed security scheme consists of two major elements: (1) Group-based Key Management and (2) Dynamic Symmetric Key Cryptography (DSKC).

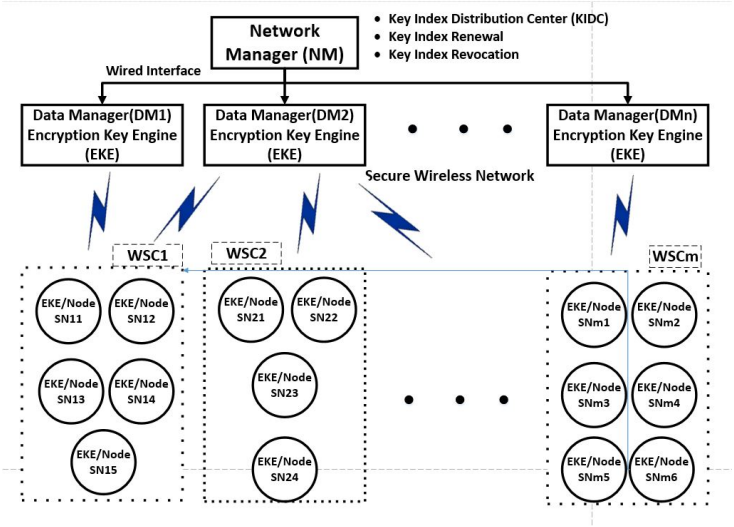


Figure 6.1: Security Architecture of the Proposed Solution

Figure 6.1 shows the security modules executed in each of the network elements. The network manager acts as the Key Index Distribution Center (KIDC). It generates the key index sequence, which we will henceforth refer to as the Initialization Vector Sequence (IVS) (see Figure 3). The network manager is also responsible for distributing the IVS and handling key renewal, based on a group-based key management scheme as described in Section 6.3. Cryptographic keys are generated by the Encryption Key Engines (EKEs) running on data managers and wireless sensor nodes. The EKEs use a symmetric key cryptography algorithm, which is described in Section 6.5. These cryptographic keys are generated from a pseudo-random sequence of significant periodicity. The sequence remains the same on both the transmitting and receiving ends. In an encrypted message, the transmitter sends the index of the pseudo-random number in the sequence. The pseudo-random number sequence generator is the same on both sides and uses the same seed argument. The transmitter sends only the index of the pseudo-random number within the sequence that was used as the key. The receiver then selects the same random number from the generated sequence, corresponding to the index. An XOR operation is then carried out for both encryption and decryption operations.

Due to the nature of the communication link, it is necessary to correctly receive the IVS at the receiving end. Therefore, a checksum is added to the message to ensure the correct reception of the IVS. The receiver constantly checks the index to ensure it matches the key sequence as per the EKE. If the index is incorrect, the receiver ignores the message and continues to do so until it receives the correct index within a specified threshold number of attempts, known as the look-ahead threshold (T1). If this threshold is crossed, the receiver declares a node attack. Upon receiving a message with the correct index, the re-

ceiver triggers the retransmission of messages for previously received incorrect indices. For a given incorrectly received index, the receiver requests retransmission a defined number of times, known as the retransmission threshold (T2). If the receiver fails to receive the correct index after T2 retransmissions, it declares a node attack. This approach reduces retransmission overhead on the network, thus improving data throughput. The "wait and watch" strategy reduces the receiver's vulnerability to adversarial attacks, even without an intrusion detection system in place. Since the proposed cryptographic scheme generates keys dynamically, it is storage-efficient and effective on resource-constrained computing platforms.

6.3 Key Management

Key management is a significant design factor for an effective security scheme. Marcos et al. [101] provide a detailed review of state-of-the-art key management algorithms for wireless sensor networks, comparing them based on qualitative metrics that are important for resource-constrained applications. The review also qualitatively analyzes the resilience of each discussed algorithm for key management. Considering a desirable connectivity level and network size, a group-based deployment scheme is proposed for the current security architecture. Figures 6.3 and 6.4 provide a schematic representation of secure transmission of the IVS. The proposed key management scheme includes key distribution and renewal algorithms.

In a particular WSN installation, there are n data managers and m wireless sensor clusters (WSCs), with $m > n$. The number of sensor nodes in each cluster is variable, and the network manager determines these numbers during the system initialization phase. It should be noted that, based on signal strength variations, a sensor node may migrate from one WSC to another during the system operation phase. This dynamic reconfiguration of the network occurs under the supervision of the network manager to address the failures of different network elements.

6.3.1 Distribution of IVS

We have employed a group-based key distribution scheme in the proposed wireless network. The KIDC transmits a set of key indices in the form of an IVS to all the data managers over the wired network. The data managers securely send a portion of the IVS to the sensor nodes in the attached WSCs. The EKEs running on the data managers and sensor nodes use the key indices to dynamically generate the cryptographic keys. The EKE generates a cryptographic key sequence iteratively. The IVS is generated from an initial random but deterministic sequence, which has a finite periodicity bounded by the bit order of the processing hardware. The IVS is distributed among multiple data managers, with each data manager receiving only a subset of the complete IVS for its respective sensor node cluster (as shown in Figure 6.2).

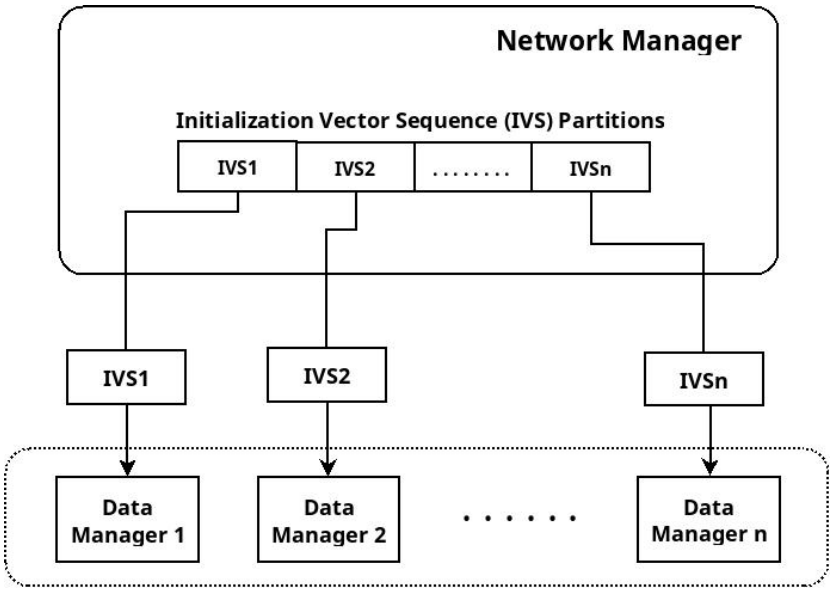


Figure 6.2: Distribution of the Initialization Vector Sequence (IVS)

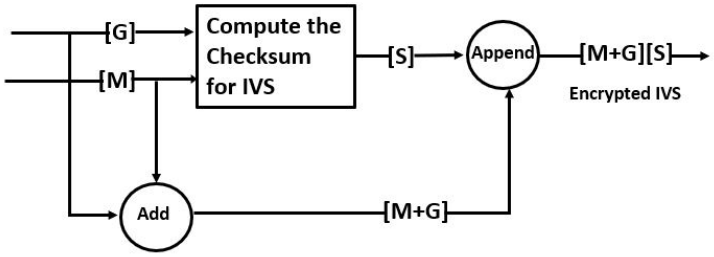


Figure 6.3: Encryption of IVS

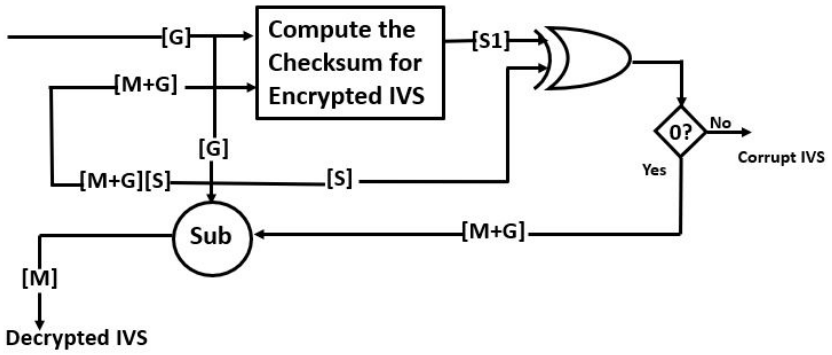


Figure 6.4: Decryption of IVS

In the group-based key distribution scheme, the i^{th} data manager receives a portion of the IVS comprising of N unique random numbers, such that

$$N = T/n \tag{6.1}$$

Where, $T =\mid IVS \mid$ and n is the number of data managers in the network. Let, IVS_i and IVS_j be the IVS partitions allocated to data managers labeled i and j respectively. In this context, the group-based distribution can be formally defined as

$$IVS_i \cap IVS_j = \varnothing \tag{6.2}$$

Where, $i \neq j$. Since, cryptographic keys are derived from the IVS and keys within a node cluster are generated from its own partition of IVS. Therefore, these keys are unique to each cluster. However, within a single cluster, all sensor nodes share the same set of cryptographic keys.

In comparison to network and pairwise distribution methods, group-based distribution offers the advantage of reduced key storage requirements and scalability, allowing for the accommodation of additional nodes in the network. Moreover, if a single node cluster is compromised due to an attack, it does not affect the other clusters in the network. Therefore, the impact of the attack is localized and confined to a subset of the network, while the rest of the network remains protected. The proposed key management algorithm ensures the secure transmission of IVS.

Assuming that the wired communication between the network manager and the data manager is secure as per the DO-355 standard for data confidentiality, integrity, and availability of aircraft networks [102], the confidentiality of the IVS transmission is primarily required for the wireless link between the data managers and sensor nodes. Before transmitting the IVS to the nodes, each data manager encrypts its corresponding IVS with a common secret key (the generator polynomial) that is known to both the data managers and the sensor nodes. Let us consider a fixed generator polynomial G, which is used to

calculate the checksum S for a given message polynomial M (the IVS partition). The formal definition of the checksum is as follows with q as the polynomial quotient.

$$M = Gq + S \tag{6.3}$$

Because of the linearity of equation 6.3, S remains same for an altered message M' defined as:

$$M' = M + G \tag{6.4}$$

Substituting the value of M in equation 6.4 we have,

$$M' = Gq + S + G \tag{6.5}$$

or,

$$M' = G(q + 1) + S \tag{6.6}$$

At the receiving side the same generator polynomial G is used to compute checksum for M'. If M' is not further tampered during transmission, then the computed checksum $S1$ will be the same as S appended along with the encrypted IVS. If the message M' is not tampered, then G is used to decrypt M' (subtract G from M'). Figure 6.4 shows retrieval of original message (IVS) at the receiving end. However, for a transmission error which changes the message polynomial in a manner $M + (2^jG)$, $0 \leq j \leq$ degree of M, the error may not be detected at the receiving end. To counter this issue, the IVS or the index sequence is chosen as a monotonically increasing function at the design stage. Hence, the erroneous IVS can still be detected by the nodes if they are not in expected sequence to the last one received. The incorrect IVS can be extrapolated to the next in sequence expected with a probability of 50% that the corrected IVS may not be proper. This is because in case there is a packet loss during transmission, the subsequent IVS transmitted may be shifted to a different index than what is expected. Therefore, the IVS encryption using generator polynomial is robust even against non-detectable transmission errors.

6.3.2 Key Renewal Strategies

Key renewal is a critical factor that determines the confidentiality strength of a cryptographic security protocol. It involves the generation of new keys in the event of either a compromise in the network or the expiry of the old keys. Ge et al. [103] extensively analyze existing key renewal mechanisms used in wireless sensor networks. The survey primarily discusses the challenges associated with both distributed and centralized key renewal schemes. However, the prior methods reported in this survey involve a deployment strategy for keys (in the case of symmetric keys) that requires prior knowledge of the network topology. This becomes particularly challenging in the context of deployment within an aircraft's wireless network, as the intra-aircraft network topology can be highly complex and dynamic due to network self-recovery and management

mechanisms. Moreover, the key renewal algorithms must be scalable. In this thesis, we propose a key renewal scheme that combines both distributed and centralized approaches for key renewal.

The KIDC module performs a two-stage key renewal process. This renewal scheme consists of local control of the keys generated within a cluster and global control over the total set of keys across the network. Local renewal is triggered when a key sequence expires within a cluster, while global revocation occurs when an intrusion or node compromise is detected in the network. However, the mechanism for detecting intrusion or node compromise is beyond the scope of this thesis. The two-stage renewal process allows communicating nodes to renew keys in a distributed manner, with no need for knowledge of other nodes in the network. In the event of an intrusion, centralized control is used to manage the renewal of keys. Figure 6.5 shows a representative diagram for the corresponding key renewal method.

1. At the global scope, the current key set of each data manager is shifted one position to the right in a circular fashion. Each data manager (or cluster coordinator) receives a new key set from its left neighbor, while its own key set is passed to its right neighbor. To determine its left and right neighbors, each data manager uses the network identifiers defined in a network deployment matrix, which is provided by the network manager during the network initialization phase.

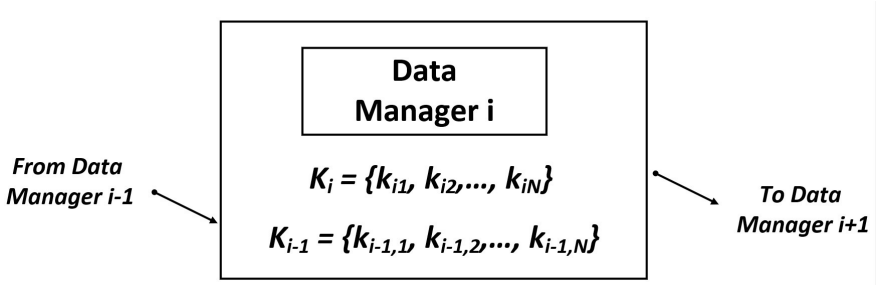
   For the i^{th} data manager, equation 6.7 and 6.8 respectively show the identity of the data manager to which it sends its own key set and the identity of the data manager from which it receives its new key set.

$$\text{To Data Manager} = \begin{cases} 1, & \text{if } i == n. \\ i+1, & \text{otherwise.} \end{cases} \tag{6.7}$$

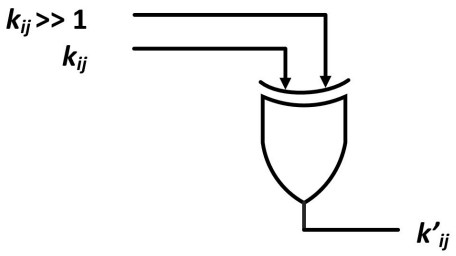
$$\text{From Data Manager} = \begin{cases} n, & \text{if } i == 1. \\ i-1, & \text{otherwise.} \end{cases} \tag{6.8}$$

2. At the local scope of renewal for the i^{th} data manager, each key $k_{ij} \in K_i$ for $1 \leq j \leq N$, is first right shifted circularly by 1 bit ($k_{ij} \gg 1$) and then XOR-ed with its old value k_{ij} to generate the new value k'_{ij}.

The two-stage key renewal scheme allows for case-dependent index renewal. The proposed method is suitable for a multi-rate sensor network with different data sampling rates. For instance, a fast cluster consisting of sensors transmitting at a higher data rate may quickly consume its allocated set of keys and thus request renewal. Local control avoids renewing the entire key sequence across the network, saving the need to redistribute new key indices or IVs to all clusters. A slower cluster, on the other hand, will have a lower frequency of local key renewals. This reduces the overhead of key management on network throughput and effectively utilizes the channel capacity.



(a) Global Scope



(b) Local Scope

Figure 6.5: Key Renewal Strategies

Global renewal, however, is performed when a sensor node in any cluster is attacked. Renewal across the network eliminates the need for local renewal at the data manager level, avoiding unnecessary computation. As a result, the global renewal algorithm does not impact the delay in data reception at the data manager, and data synchronization is also unaffected.

6.4 Resilience Analysis

Resilience is a metric that is typically used to analyse the security strength of a key management scheme. The resilience of a key management scheme represents the probability that a secure connection between any two nodes, A and B, is not compromised when x nodes (different from A and B) are captured. The higher the resilience of a key management scheme, the more secure the network is. Resilience is denoted as $P_r(x)$, and formally defined as follows [104].

$$P_r(x) = 1 - P_c(x) \tag{6.9}$$

where, $P_c(x)$ represents the probability that a link is compromised when x nodes are captured. $P_c(x)$ is defined by the following conditional probability:

$$P_c(x) = P\{L_c \mid C_x\} \tag{6.10}$$

where, L_c is the event in which a link is compromised and C_x is the event in which x nodes are captured. Marcos et al [101] presents a detailed analysis of resilience for different key management algorithms. Mathematical expressions have been defined for computing the $P_c(x)$ values for a given key management algorithm. However, the WSN architecture described in section 6.2 consists of sensor nodes which communicate only with the data manager and not among themselves. The principles defined in [101] are purely based on peer-to-peer communicating elements without having any communication constraints. Hence, there exists multiple links between any two given nodes. For the WSN architecture proposed in this section, we take a slightly different approach in analysing the resilience of group based key management scheme described in section 6.3.

Let us consider a cluster of s number of sensors connected with a data manager in a bipartite mode (i.e. no sensor node directly communicates with another, and that sensor nodes communicate only with the data managers). Therefore, computing the $P_r(x)$ for the cluster will determine the resilience of the communication link between the data manager and the cluster. The key pool K_i for the i^{th} data manager remains same for all the sensor nodes in the attached cluster. Since, the local scope of the key renewal happen only at the sensor cluster level, a single node compromise may be sufficient to compromise the entire cluster till K_i gets renewed by some nodes which are not yet directly compromised. Hence, a successful compromise of the complete cluster may be

constrained by the number of nodes which generate a new sequence K_i' from the original pool K_i.

Let us assume that x nodes have been compromised and which are preserving pool K_i for securing their data transmissions. Hence, remaining $(s - x)$ nodes may have gone for a renewal or are still resuming K_i keys. The conditional probability $P_{s-x|x}$ that none of the uncompromised nodes have performed key renewal and are vulnerable given x nodes are already compromised is defined as follows.

$$P_{(s-x|x)} = (\frac{1}{2})^{\frac{s!}{(s-x)!x!}} \tag{6.11}$$

The exponent is defined as number of unique ways in which $(s - x)$ nodes out of s nodes can be vulnerable to attack after the direct compromise of x nodes in the cluster.

Hence, the probability $P_r(x)$ that at least one node has gone for a renewal is:

$$P_r(x) = 1 - P_{(s-x|x)} \tag{6.12}$$

Substituting $P_{(s-x|x)}$ in equation 6.12 with equation 6.11, resilience of the key management algorithm can be defined as:

$$P_r(x) = 1 - (\frac{1}{2})^{\frac{s!}{(s-x)!x!}} \tag{6.13}$$

Let us now consider the impact of key renewal at the global scope, which is triggered upon detection of intrusion in the network. Consider that, total X number of sensor nodes exist in the network with an average cluster size of s nodes. Therefore, expected number of clusters w is defined as

$$w = X/s \tag{6.14}$$

Since, compromise of a node cluster is independent of compromise of another - the total probability P_w that all of the clusters get compromised and the encryption key chain exposed to the attacker is defined as:

$$P_w = \prod_{i=1}^{w} p_i \tag{6.15}$$

Where, p_i is the probability of successful attack on the i^{th} cluster. Since a cluster may be considered to be fully compromised if the attacker is capable of extracting the key pool K_i by compromising the nodes either directly or indirectly, p_i is the same as $P_{(s-x|x)}$ for the i^{th} cluster. Hence, P_w can be redefined as:

$$P_w = \prod_{i=1}^{w} P_i(s - x \mid x) \tag{6.16}$$

Substituting the value of $P_c(x)$ in equation 6.16 we get the total probability of network failure $P(n)$, due to node compromise in all the clusters as:

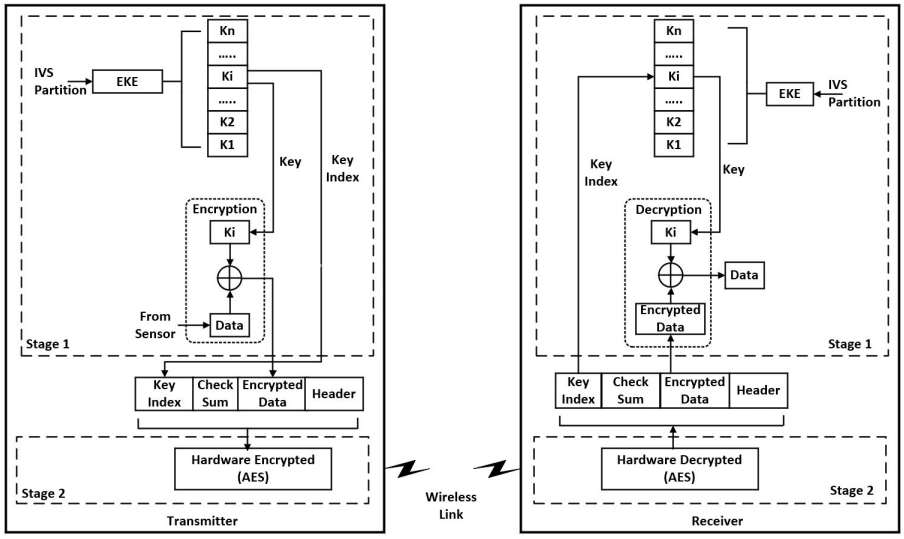


Figure 6.6: Two-Stage Cryptography Scheme

$$P_w = \prod_{i=1}^{w} (\frac{1}{2})^{\frac{s!}{(s-x)!x!}} \tag{6.17}$$

Hence, resilience for the overall key management algorithm $Pr(x)$ is enhanced to

$$P_r(x) = 1 - P_w \tag{6.18}$$

Substituting the value of P_w in equation 6.18, $P_r(x)$ can be defined as:

$$P_r(x) = 1 - \prod_{i=1}^{w} (\frac{1}{2})^{\frac{s!}{(s-x)!x!}} \tag{6.19}$$

Equation 6.19 clearly brings out the effectiveness of the two-stage key renewal algorithm which can make the network security robust to node compromise.

6.5 Cryptographic Algorithms and Protocols

We have employed a two-stage cryptography scheme to provide an optimized and robust security framework for intra aircraft WSN. The two stages are: (1) dynamic symmetric-key cryptography (DSKC) and (2) hardware-based cryptography. The schematic diagram in figure 6.6 shows this two-stage cryptography scheme.

6.5.1 Dynamic Symmetric-Key Cryptography

The dynamic symmetric-key cryptography scheme uses the same set of keys on both the transmitting and receiving ends. In this scheme, cryptographic keys are generated from a pseudo-random sequence with significant periodicity, and the seed is a dynamically generated number. The key sequence remains the same on both the transmitting and receiving ends. In a message, the transmitter sends the index of the pseudo-random number used as the key along with the encrypted data. The receiver then picks the same pseudo-random number from the generated sequence to use as the key for decryption.

Both the encryption and decryption process involve simple XOR operation - hence, they are faster as compared to other techniques that use integer arithmetic.

Encryption key engines (EKEs) located in the sensor nodes and the data managers (shown in Figure 6.1), use the respective IVS chunks received from the KIDC to generate the encryption keys dynamically. Formally the key generation algorithm KG can be defined as:

$$KG : IVS_i \rightarrow K_i \tag{6.20}$$

where, $K_i \in Z$ is the set of encryption keys generated by KG using IVS_i as the input. Let IVS be a pre-determined sequence divided into equal length chunks such that $IVS_i \neq IVS_j, \forall i \neq j$. KG being a deterministic algorithm for generating random numbers, $K_i \neq K_j, \forall i \neq j$. Hence, given IVS_i, KG will be able to generate a unique K_i.

In our scheme, we have chosen Schrage's congruential method [105] as the base for generating pseudo-random numbers to implement KG. This algorithm is effective for implementation on low-powered hardware with memory constraints. The basic pseudo-random generator is modified by introducing a pre-determined seed number sequence to improve the periodicity of the computed random numbers. Below, we provide an analysis of the irreproducibility of the encryption keys generated using Schrage's algorithm as the foundation. The analysis begins with a brief introduction to Schrage's algorithm.

It is often desirable to have a random number generator that is independent of the underlying computing hardware. Schrage proposed an algorithm for multiplying two 32-bit integers modulo a 32-bit constant, without using any intermediate values larger than 32 bits. In aircraft scenarios, where most sensing applications run on devices that are resource and power-constrained, such an approach is effective for random number generation. Equation 6.21 is a basic congruential method for generating random numbers.

$$K[i] = (K[i-1] \times S[i]) \bmod M \tag{6.21}$$

where, M is a large prime number known as the modulus. S is the seed number which in the present scope of the thesis is obtained from the IVS. Schrage defined the value of divisor M as follows.

$$M = a \times q + r \tag{6.22}$$

We have chosen the values for the parameters a, q and r as: $a = 16807$, $q = 127773$ and $r = 2836$. In order to increase the degree of randomness, we have introduced a variable definition of the divisor M in equation 6.21

$$M[i] = S[i] \times q + r \tag{6.23}$$

With $S > 0$ the order of magnitude of M is still preserved and since S is a controlled deterministic sequence in itself the value of M remains deterministic. Hence, the random number generation is transformed into a pure discrete sequence.

Considering $r \ll q$, equation 6.21 can be equivalently expressed [106] as follows:

$$K[i] = S[i] \times (K[i-1] \bmod q) – r \times \frac{K[i-1]}{q} \tag{6.24}$$

Now, Let us analyze $K[i]$ with respect to an exponential seed S. The IVS uses a Fibonacci sequence for generating the initial seed numbers in a computationally simple manner. In order to analyse the effect of a Fibonacci seed to equation 6.24 we need to describe the Fibonacci sequence in parametric form. Using the principle of least squares, the Fibonacci series may be approximated using an exponential series as defined in equation 6.25.

$$F[i] \equiv \theta_1 e^{i\theta_2} \tag{6.25}$$

Where, $i > 0$, $i \in Z$, $\theta_1 < 1$ and $\theta_2 < 1$. Equation 6.25 is a discrete approximated sequence for the Fibonacci sequence $F[i]$. Substituting the value of $F[i]$ in place of $S[i]$, equation 6.24 can be redefined as:

$$K[i] = \theta_1 e^{i\theta_2} \times (K[i-1] \bmod q) - r \times \frac{K[i-1]}{q} \tag{6.26}$$

Since $r/q < 1$, the second component can be ignored.

Considering the periodicity of the random sequence to be t, $K[i-1] < q$, $\forall i \leq t$ and hence equation 6.26 can be upper bounded as follows.

$$K[i] = \theta_1 e^{i\theta_2} K[i-1] \tag{6.27}$$

It is evident from equation 6.27 that the exponential seed is governing factor in the key sequence generation. Considering the values of θ_1 and θ_2 the autocorrelation coefficient $\Phi KK[p]$ for $K[i]$ is computed as an approximated function defined in equation 6.28.

$$\Phi KK[p] \approx \frac{p\theta_1}{1-\theta_2} \tag{6.28}$$

Where, p is the time delay for computing the autocorrelation. Hence, the key sequence $K[i]$ becomes unpredictable as $p \to \infty$. Hence, $K[i]$ will be uncorrelated if sampled at p intervals. Moreover, it is evident from equation 6.27,

the seed sequence is detectable by an external entity, which observes only the cipher-text, if and only if θ_1 and θ_2 are solved with respect to the periodicity t. Hence, it is computationally intractable to reproduce the encryption keys generated using equation 6.26.

6.5.2 Hardware-Based Cryptography

The hardware-based cryptography scheme utilizes the AES cipher engine embedded in the Atmel ATMEGA-128 hardware module. The encrypted sensor payload from Stage 1 is further encrypted by the Atmel cryptography module using a static AES key. Since this key is programmed once and remains consistent across all AES engines in the WSN, there is no need to transmit encryption keys for the hardware-based scheme.

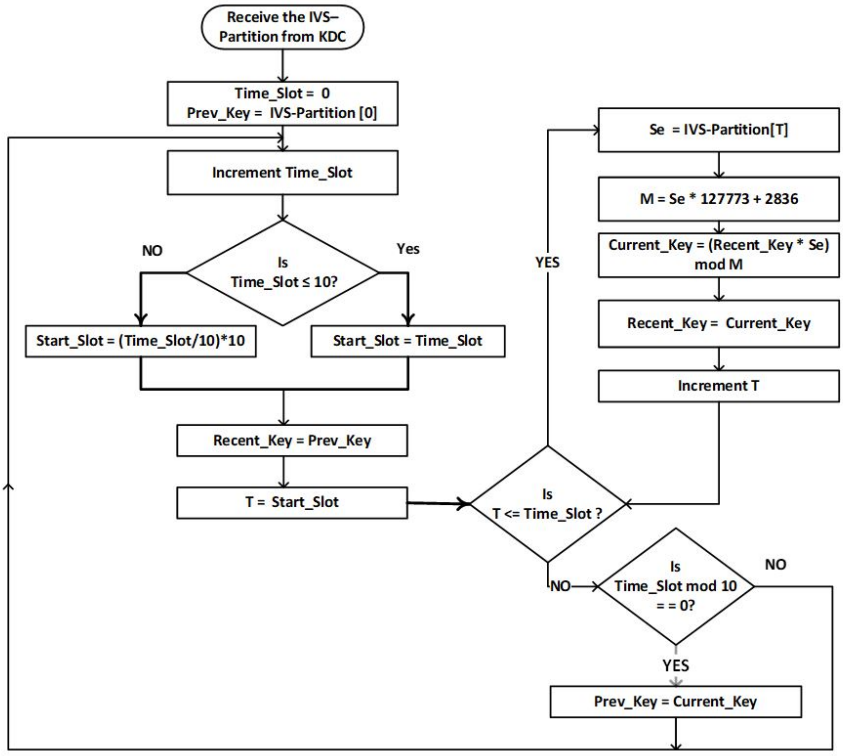


Figure 6.7: Flow Chart of Cryptographic Key Generation

Algorithm 1 shows a naive implementation of the proposed key sequence generation based on Schrage's method. Clearly, the algorithm exhibits linear time complexity. Since the algorithm iterates over the value of the key index, it is evident that it iterates more times for larger key indices, which occur at

Algorithm 1 Dynamic Symmetric Key Cryptography Algorithm

Require: IVS, Key_{index}
  Key_{pre} = Computed from Schrage's Method
  while $Key_{index} > 0$ **do**
    Fib = IVS[Key_{index}]
    $Fib = (Fib \ \% \ 65535) + 1$
    $Key_t = (Fib \times 65534) \% \ 65535 + 1$
    $Key_{algo} = (Key_{pre} \times 16807) \ \% \ Key_t + 1$
    $Key_{pre} = Key_{algo}$
    $Key_{index} = Key_{index}$ - 1
  end while
  return Key_{algo}

successive time slots. This may influence the network throughput. Therefore, the naive algorithm needs to be optimized.

The basis of the optimization of the key generation scheme is to reduce the number of iterations required for computing key values as the time slot count increases. The key generation algorithm has been modified based on Scharge's method, as discussed so far. Figure 8 shows the flowchart of the optimized encryption algorithm. This algorithm computes a pseudo-random number generated using the linear congruential method, where the periodicity factor M is calculated randomly using values from the IVS. This ensures an increased period for the PRN sequence even for 8/16 bit hardware.

To compute the encryption key for the current time slot, the EKE algorithm uses the previous encryption key generated in the highest integral multiple of 10 time slots prior to the current time slot as the seed value. For example, if the key for Time Slot 23 needs to be computed, the key generated at Time Slot 20 will serve as the seed. The encryption key is then computed in 3 iterations starting from the seed. Thus, the optimized algorithm limits the number of iterations at each time slot to a maximum of 10, using the last recorded encryption key value, as shown in the flowchart. Since the algorithm requires the storage of only a single key, it also ensures storage efficiency.

Typically, the wireless nodes execute their software on embedded microprocessors or microcontrollers, where data is stored in EEPROM or NVRAM for subsequent use by the algorithm. The proposed algorithm uses both local and global storage in RAM and EEPROM, which helps prevent data leaks due to malicious access of memory locations in EEPROM in case a node is compromised.

The periodicity of storage for previous key values is determined by analyzing the autocorrelation of the encryption key sequence. To compute the autocorrelation, the key values are correlated with themselves at different sampling intervals (time lags).

Figure 6.8 shows the decrease in the correlation coefficient value to a minimum of zero as the time lag increases. Figure 6.9 provides a higher-resolution

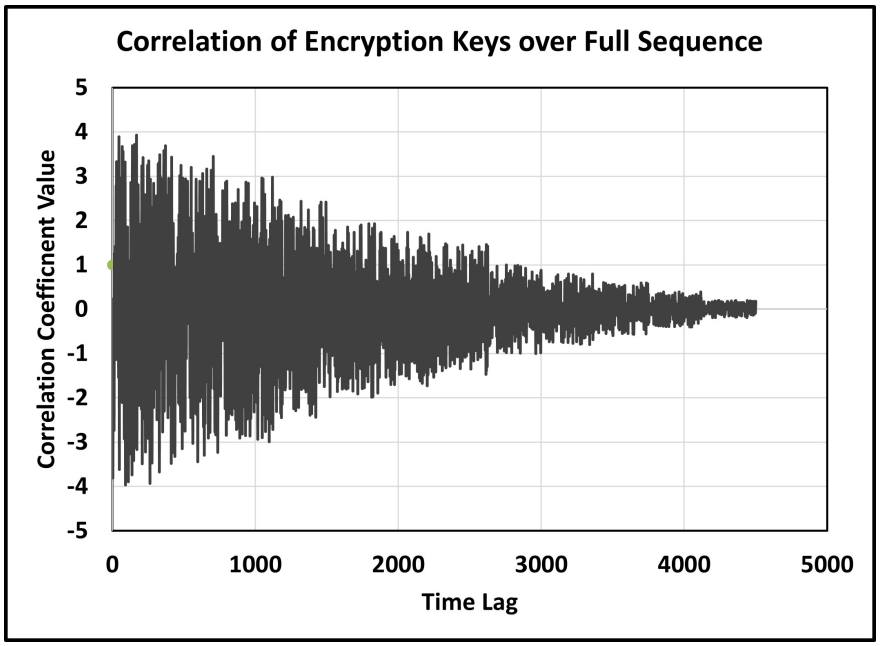


Figure 6.8: Correlation of Encryption Keys over Full Sequence

view of the correlation coefficient within a time lag of 50. The low correlation of the encryption keys reduces the probability of predicting a value based on another value in its close vicinity within the sequence. It is evident from Figure 6.9 that the correlation between the encryption keys is lowest for time lags less than 10. Therefore, 10 is the lowest time lag at which a very low correlation coefficient value is obtained.

Considering a throughput-aware security mechanism for wireless communications inside aircraft, the following performance requirements have been established for the proposed cryptographic scheme:

1. To demonstrate a minimum key lifetime of one hour for a given set of unique keys.
2. To demonstrate the security overhead on 32-bit hardware.
3. To demonstrate a computing overhead of less than 1% of the message transmission time.

In the next section, we provide a statistical analysis of the generated keys and the computational overhead of the overall security scheme. We also discuss the performance of the scheme based on two metrics: PDR (Packet Delivery Ratio) and EED (End-to-End Delay), as defined by Tomic et al. [52].

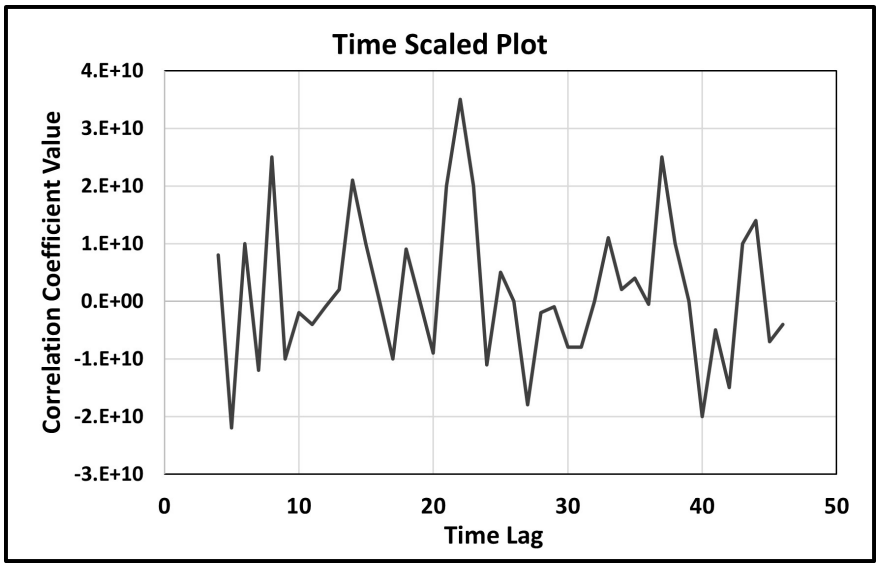


Figure 6.9: Time Scaled Plot

6.6 Performance Evaluation

We evaluated the performance of the key management and cryptographic schemes in two steps. In the first step, we tested the network manager, data manager, and wireless sensor cluster functions in a laboratory-scale experimental setup, as shown in Figure 6.10. The following components were used to implement the different functions:

1. A COTS desktop computer hosts the network manager functions, including network configuration, network arbitration and monitoring, and key management. The key management function comprises the following sub-functions: key initialization vector sequence generation, key index distribution, key renewal, and key revocation.

2. The Atmel ATMEGA-128 hardware hosts the data manager functions, which include EKE, DSKC, data aggregation from multiple sensors, and interfacing between the network manager and sensor nodes.

3. The TI CC2650 16-bit evaluation hardware hosts the functionality of a wireless sensor cluster, including EKE, sensor nodes, and DSKC.

Both the Atmel ATMEGA-128 and TI CC2650 hardware supports ISM 2.4 GHz Band with an integrated IEEE 802.15.4 MAC protocol. We have selected a beacon enabled transmission protocol for evaluating the performance of the proposed security scheme. The key management scheme is carried out on

beacon enabled TDMA protocol with guaranteed time slots (GTS) mechanism [10].

In the following, we describe the communication sequence carried out to implement the distribution of IVS:

Step1: IVS is generated from a Fibonacci sequence within the network manager and is distributed via the data managers to the respective WSC during the contention access period (CAP) of a beacon cycle.

Step2: IVS partitions are transmitted as a one-to-one dedicated communication from a data manager to a WSC.

Step3: WSCs encrypt their respective message using keys generated by the EKE. The encrypted message is sent to the data manager along with the value of the current time slot.

In the next step, the algorithms are tested in the final configuration, as per the network architecture shown in Figure 3.3. In the test environment, the network manager functionalities are hosted on dedicated system hardware, which is part of the avionics line-replaceable unit (LRU) in the cockpit. The data manager functions are hosted on Atmel ATMEGA-128 hardware, supporting the ISM 2.4 GHz Band with an integrated IEEE 802.15.4 MAC protocol [10]. The sensor package includes multiple sensors, such as temperature, current, and pressure sensors, which communicate through integrated transceiver modules operating at 2.4 GHz. In Section 6.6.1 , we present a statistical analysis of the cryptographic keys generated by the symmetric key cryptography algorithm. In Section 6.6.2, we describe the computational effectiveness of the cryptographic algorithm, along with its performance verification against the metrics packet delivery rate (PDR) and end-to-end delay (EED), as defined by Tomic et al. [52].

6.6.1 Assessment of Encryption Key Strength

In this section, we describe the tests of the statistical characteristics of the encryption keys generated by the EKEs using the key generation scheme outlined in Section 6.5. The statistical distribution of the randomly generated sequence of keys determines the probability of how quickly an attacker can decipher and possibly corrupt the sequence using a parallel cryptosystem. This ensures the robustness of the proposed encryption algorithm against adversarial attacks.

Figure 6.11a shows the histogram plot of the generated encryption keys. The largest number of keys are generated with values less than 10,000. However, the histogram approximates an exponential distribution for values greater than 40,000. The frequency of encryption keys for values greater than 40,000 is less than 100 out of the 3,000 keys generated, which accounts for only 3%. Therefore, even the identification of an approximated exponential distribution can effectively recreate only 3% of the original key sequence. This reduces the potential for an attack on the proposed cryptosystem to only 3% through key regeneration by the attacker.

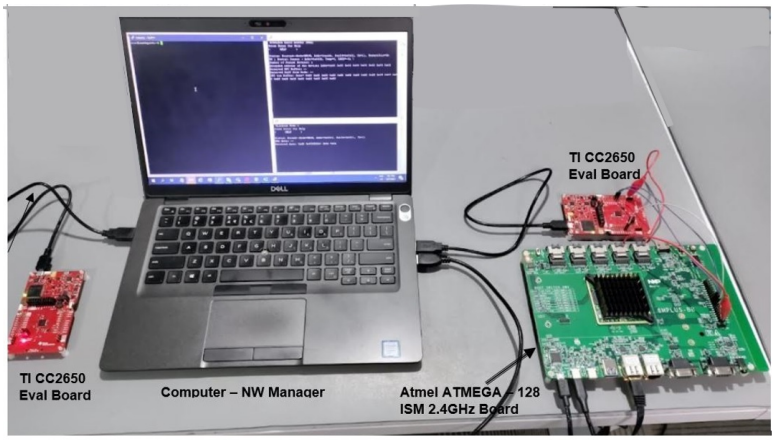


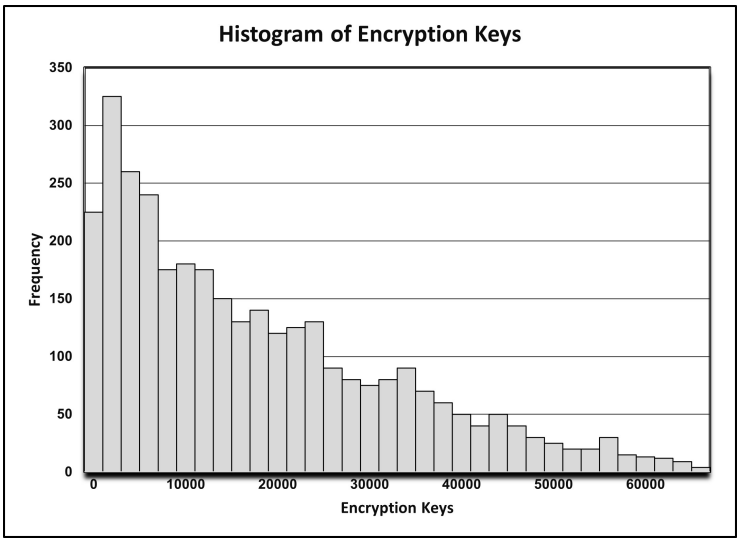
Figure 6.10: Laboratory Scale Experimental Setup

The QQ-Plot analysis reveals 95% confidence interval values or matches for the encryption keys with an exponential distribution as shown in Figure 6.11b. The exponential distribution is plotted as a straight line and the encryption keys are plotted in boldfaced line. The key values from 1000 to 80000 are having a close match with the percentage exponential distribution between 5% - 95% as indicated along the vertical axis.

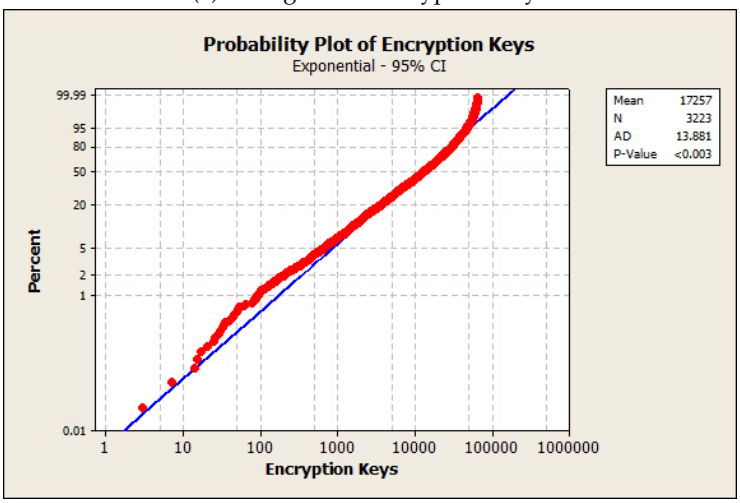
6.6.2 Analysis of Computation and Network Overhead

In our experiments, both the naive and optimized encryption algorithms are executed on the Atmega-128 hardware with a 16 MHz processor frequency. The optimal execution time for the binary code is 27 μs. Execution time is estimated by counting the CPU cycles consumed by the code. The overhead due to encryption is 0.08% of the time required to transmit a maximum of 127 bytes on the IEEE 802.15.4 channel, at an average throughput of 22 Kb/s. Table 6.1 shows the detailed analysis of the computation time required for the optimized encryption algorithm at the hardware level.

The naive code resulted in varying turnaround times over the wireless channel. Since the naive algorithm iterates more times for high values of key indices than the optimal algorithm, the time required to compute encryption key values increases monotonically, then resets when the value overflows the hardware's bit capacity. This increases the turnaround time for a packet on the network. As a result, the data throughput for the network decays exponentially in a periodic manner, as shown in Figure 6.12a. In contrast, the optimal algorithm reduces variations in the turnaround time, and the slope of the ramp is smaller. As a result, the throughput of the network improves, as shown in Figures 6.12c and

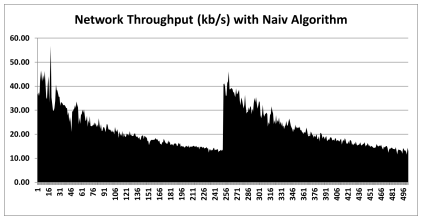


(a) Histogram of Encryption Keys

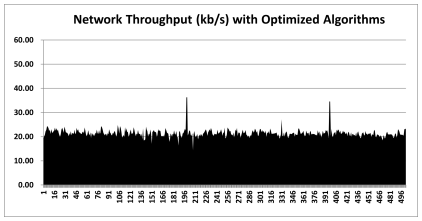


(b) QQ-plot of Encryption Keys

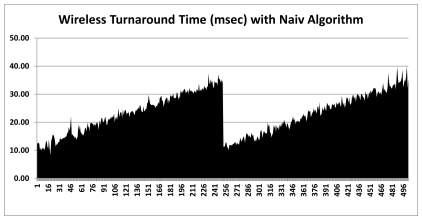
Figure 6.11: Statistical Analysis of Encryption Keys



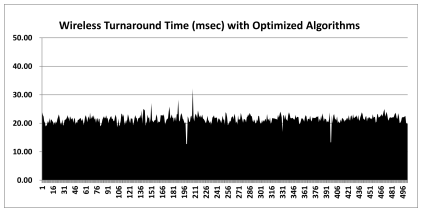
(a) Network Throughput of Naïve Algorithm



(b) Network Throughput of Optimized Algorithm



(c) Wireless Turnaround Time of Naïve Algorithm



(d) Wireless Turnaround Time of Optimized Algorithm

Figure 6.12: Analysis of Computation and Network Overhead

6.12d.

Table 6.1: Machine Level Execution Time Analysis of the Cryptographic Scheme

Computing Analysis	Particulars
Machine cycles (Cycles)	434
Machine frequency (F)	16 MHz
Computation time (P)	Cycles/F = 27 μs
Wireless transmission time (T)	20 ms
Time overhead	$(P/T) \times 100$ = 0.135%

Table 6.2: Analysis of Encryption Algorithm against PDR and EED

Testing Scenario	PDR (%)	EED (ms)
Close Vicinity - 70 bytes transmission	99.83	29.33
Far- 127 bytes transmission	93.57	30.28
Far - 127 bytes transmission (Interference)	85.53	28.19

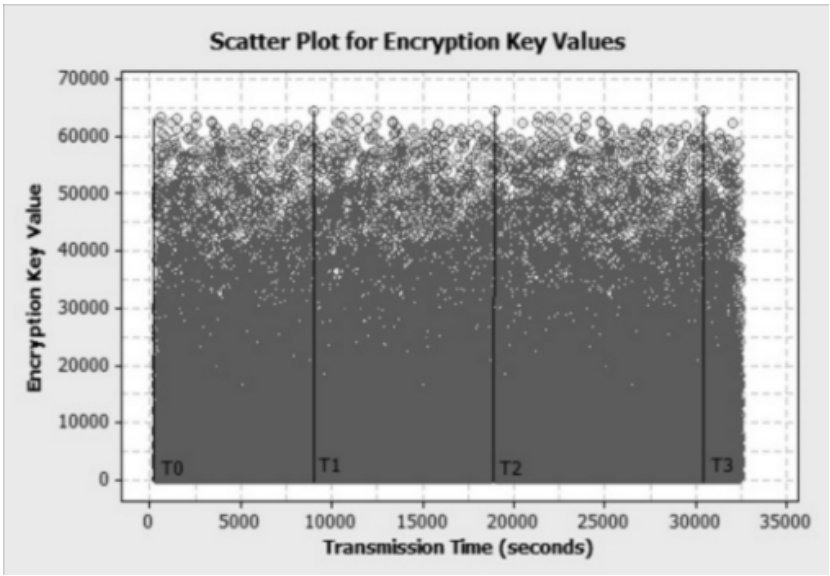


Figure 6.13: Estimated Lifetime of Unique Key Sequence

From a different perspective, the lifetime of an encryption key sequence (allocated to a particular sensor cluster) determines the frequency of local key renewals at the cluster level. Therefore, it is important to have a longer periodic span for the random sequence before renewal occurs. The proposed encryption algorithm can generate a random sequence that cycles at an interval of at least 9000 seconds (shown in Figure 6.13), meeting the minimum requirement of a one-hour key lifetime. The size overhead due to encryption of the message is shown in Figure 6.14.

Since the encryption key is a 16-bit value, 8 bits may remain unused when encrypting an 8-bit message. In this case, 8 bits of the encryption key, along with 16 bits of the IV (Key Index), will be overhead due to the encryption process. However, in the case of a 16-bit message, the overhead consists only of the 16 bits of the IV. Therefore, the encryption method meets the second performance requirement as well. Table 6.2 presents an assessment of the cryptographic scheme with respect to the PDR and EED metrics. The values indicate that the PDR is lower in interference scenarios and when there is a large distance between the wireless devices. This is primarily because the decrease in the signal RSSI, as the distance increases, results in a lower SNR.

Corruption of the IV transmitted along with the encrypted message causes the symmetric algorithm to fail in computing the correct encryption key, resulting in an incorrect extracted message. Since the computation of encryption keys is independent of the distance of separation, it does not significantly impact the end-to-end delay (EED). Moreover, as discussed earlier, the security overhead remains almost constant for all transmissions.

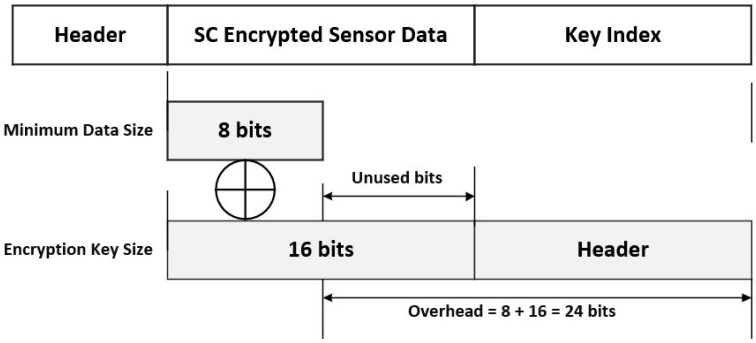


Figure 6.14: Data Overload Due to Encryption

6.7 Chapter Summary

In this chapter, we have presented and analysed a security framework for wireless intra-aircraft communication. We have described security algorithms that were evaluated as per the QoS and performance requirements for a WSN operating inside an aircraft. A group based key management has been discussed. Key renewal algorithms have been presented as local and global renewals within each sensor cluster and across the wireless network respectively. A symmetric cryptography algorithm using Scharge's congruence algorithm for a lightweight random key generation has been explained. The security framework thus presented, has been analysed in terms of security metrics like strength of encryption, resilience of key management and computational efficiency in terms of time and packet size overhead. The algorithms were tested on Atmega-128 hardware at 16 Mhz. The overall encryption overhead was found to be 0.08% of the transmission time considering a throughout of 22 KB/s over an 802.15.4 channel. Under worst case conditions of transmission, the Packet Delivery Ratio (PDR) was found to be 85% with a best case of 99.8%. Effectiveness of encryption algorithms to provide optimal network throughput even on low-end computing platform has been demonstrated. Robustness of proposed algorithms to adversarial and node compromise attacks in an aircraft scenario has been discussed.

Chapter 7

Applications of IAWSN

7.1 Introduction

As the aerospace industry advances toward sustainable aviation by embracing electric and hybrid propulsion systems, Intra Aircraft Wireless Sensor Networks (IAWSN) play a vital role in ensuring the safety and reliability of aviation. In Chapters 3, 4, and 6, we present the essential technologies required for implementing a secure, scalable, and adaptable IAWSN, which include the following:

1. A hierarchical network architecture featuring fault tolerance,
2. Communication protocols that optimize network throughput while addressing network coexistence and interoperability and
3. A security framework that employs lightweight algorithms tailored to meet the functional needs of aircraft.

The Aerospace Vehicle Systems Institute (AVSI) Working Group [81] has proposed a range of applications for both inside and outside the aircraft, utilizing various sensors to detect smoke, proximity, ice, lightning, and more, with variable data rates and types. In addition to developing Wireless Sensor Networks (WSN) for health monitoring and control applications, researchers are investigating opportunities to gradually replace the wired harnesses traditionally used for power transmission on-board aircraft with wireless solutions. In this chapter, we propose a framework and platform for two applications of IAWSN that are scalable to Wireless Aviation Integrated Communication (WAIC):

1. Integrated Aircraft Health Management (IAHM)
2. Wireless Power Transfer (WPT)

7.2 Framework for IAHM

Aircraft health monitoring utilizes onboard sensors distributed throughout the aircraft, along with data transmission and analysis, to assess the aircraft's structural condition and system performance. This monitoring process helps determine the aircraft's airworthiness, leading to improved operational safety and economic efficiency. This comprehensive approach is referred to as Integrated Aircraft Health Management (IAHM).

Currently, various groups are developing different systems and platforms for applications related to aircraft health monitoring, such as Structural Health Monitoring (SHM), Prognostics and Health Management (PHM), Aircraft Health Management (AHM), and Engine Health Monitoring (EHM). However, these applications often use a federated architecture, where data acquisition, processing, and storage are confined to individual components or Line Replaceable Units (LRUs). Consequently, fault and failure data are recorded within their respective LRUs and are retrieved during Maintenance, Repair, and Overhaul (MRO) processes using customized data interfaces. This federated approach can lead to delays in identifying component degradation and failures, which results in delays in the timely availability of spare parts required to address these issues.

With advancements in computing and communication technologies, there is an opportunity to replace the federated architecture with an Integrated Modular Architecture (IMA). In the IMA concept, each LRU would have its own internal data acquisition and processing modules, and all LRUs would be interconnected through a network. This setup would allow data and reports from all LRUs to be accessed by a centralized network manager. By leveraging advanced sensors, processors, and storage devices, real-time data and reports from LRUs can be made available for both on-board and off-board applications, including PHM, EHM, and SHM.

This integration facilitates using advanced analytical methods, such as statistical trend analysis and estimation techniques, to process data from multiple sources. These methods enable the prediction of component, subsystem, or system performance, allowing for timely failure detection and prediction both in-flight and on the ground. This proactive approach helps eliminate delays associated with only scheduled maintenance.
In this section, we have presented:

1. A qualitative analysis of existing health monitoring systems and proposed a framework and a platform for IAHM.

2. An IAWSN architecture for IMA to execute data acquisition, data processing, data fusion, and communication with capabilities to perform diagnostics, prognostics, and decision making, and communication with capabilities to perform diagnostics, prognostics, and decision-making

3. A Methodology to execute onboard diagnostics and generate in-flight warning to the crew.

4. A discussion on The benefits of advancing to IMA with IAWSN over federated architecture.

To accelerate the IAHM system, researchers have highlighted its operational and business advantages. According to the authors in [82], "the technologies associated with IAHM applications enable an aircraft to gather data from its various systems and subsystems, analyzing it to reach critical decision-making points." IAHM includes applications such as prognostics and diagnostics that facilitate condition-based maintenance for these systems and subsystems. The guidelines from a NASA report [83] emphasize that "in safety-critical domains like aerospace, IAHM must provide fault-tolerant responses, including system and subsystem reconfiguration, to prevent catastrophic failures. Additionally, it aids in planning and scheduling post-operational maintenance to prevent sudden field failures, thereby enhancing the safety, reliability, maintainability, operability, and testability of the integrated system."

7.2.1 Federated Architecture

At present, in an aircraft, there are health monitoring systems which, in their simple form, implement continuous monitoring of aircraft data in real-time through the use of dedicated sensors and software to provide information related to on-board diagnostics and off-board ground-based information for maintenance and logistics as shown in Figure 7.1.

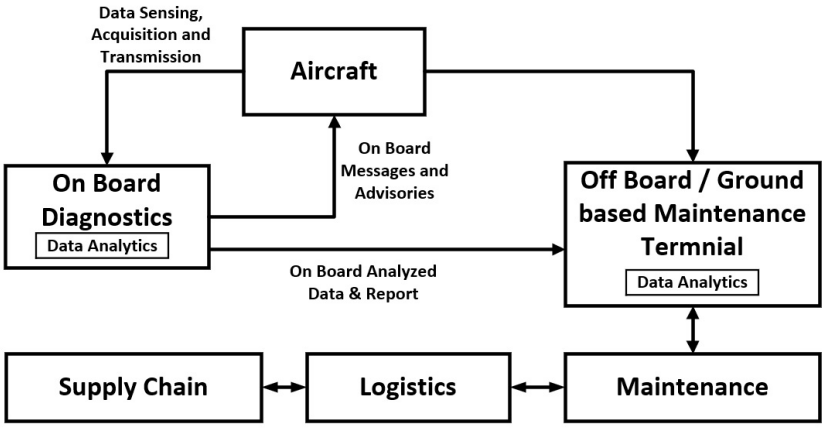


Figure 7.1: Current Scenario - Health Monitoring in Aircraft

In the existing aircraft health monitoring system, as shown in Figure 7.1, data is gathered from LRUs distributed across the aircraft in a federated structure. Within this architecture, each LRU functions as a self-contained module, hosting a dedicated application and managing its own private resources, as

illustrated in Figure 7.2. Each LRU operates autonomously, integrating its own applications, processing units, and I/O channels that communicate via a physical medium. Fault data generated by these applications is shared with other LRUs when necessary. Maintenance personnel at MRO facilities retrieve this maintenance data, which includes fault and failure information, for diagnostic analysis.

Systems are increasingly becoming more federated and distributed as greater intelligence is integrated into individual units. However, this decentralized architecture on aircraft presents challenges in visualizing the aircraft as a unified system for data collection from numerous LRUs. Consequently, it limits the ability to leverage the advantages of collective intelligence, data centralization, and large-scale data fusion. In many instances, fault and failure data are utilized only during the maintenance phase when the aircraft is grounded, restricting their potential for broader, real-time applications.

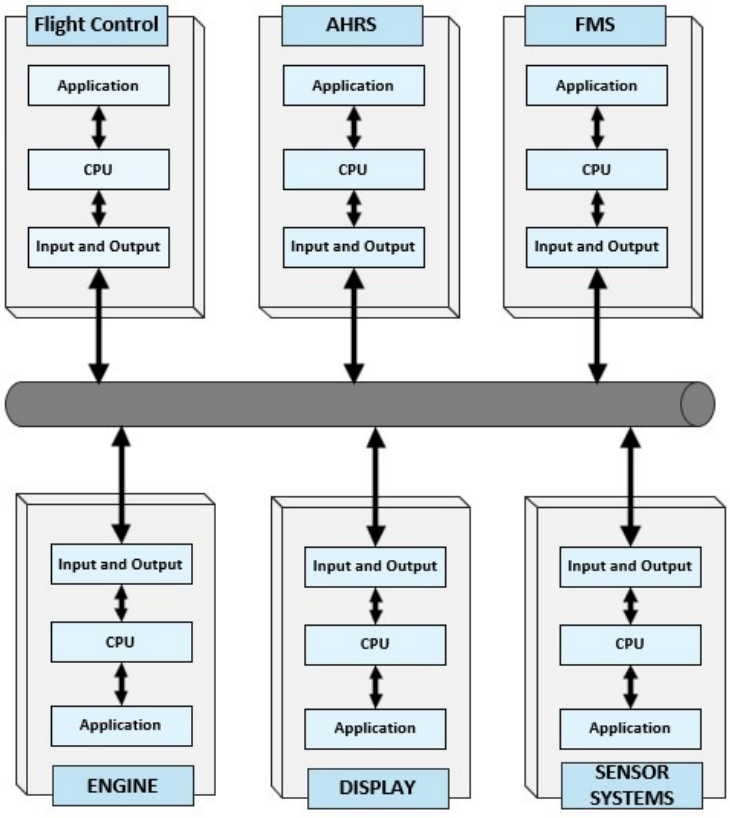


Figure 7.2: Federated Architecture in an Aircraft.

The architecture of a health monitoring system should enable seamless in-

tegration of components, subsystems, and systems to enhance interoperability and foster collaboration and shared understanding across various levels. This approach underpins the development of an Integrated Aircraft Health Management System. The OSA-CBM, open system architecture for condition-based monitoring standards [84] provides a standardized framework for information flow within a highly integrated health monitoring system. The proposed platform and framework incorporate the functional blocks of OSA-CBM while addressing the architectural requirements essential for implementing a comprehensive and unified health management system.

7.2.2 Integrated Architectural Framework

In this chapter, we have explored the factors driving the need for a distributed architectural framework in Integrated Aircraft Health Management (IAHM) and introduced the proposed Integrated Architecture. IAHM requires distributed computing resources across the aircraft, working collaboratively to enable advanced prognostics and diagnostics applications. This distributed architecture must support both onboard and ground-based systems, emphasizing the standardization of data acquisition, processing, health management, prognostics, and information sharing. Achieving this involves pluggable applications operating on similar processing platforms, configurable input/output systems, communication networks, and a flexible operating system with temporal and spatial partitioning.

Given the vast amounts of heterogeneous data—potentially reaching terabytes—IAHM demands advanced data management and mining capabilities. These capabilities extend beyond raw analytics to encompass data storage, distributed storage, and pattern recognition through artificial intelligence, neural networks, and machine learning techniques [85]. IAHM must also identify key characteristic properties whose deviations signal system anomalies, triggering alerts to notify users of unusual behavior.

In an efficient and integrated IAHM system, a distributed architectural framework serves as the core, facilitating communication and processing of extensive data across various systems and subsystems [107] [108].

we have outlined the proposed IAHM system's architectural design, as illustrated in Figure 7.3. The architecture incorporates elements of the IAWSN framework, depicted in Figures 3.9 and 6.1. Detailed discussions on the components and subsystems of this architectural framework are provided.

Sensor Cluster: The framework comprises multiple zonal clusters of wired or wireless sensor nodes that collect health data. An aircraft is divided into several zones, each with clusters of sensors dedicated to specific areas such as the fuselage, engines, cabin pressurization, control surfaces, actuators, and structural elements. Within each cluster, the sensor nodes transmit the acquired data to Data Managers wirelessly, prioritizing the data based on its urgency and the specific application requirements.

Data Managers: Zonal Data Managers are equipped with edge computing capabilities to process encrypted data locally. They analyze the incoming data

from sensor clusters to identify and prioritize relevant information based on events or deviations. The processed data is then converted into an efficient storage format as per the system's configuration. Subsequently, the data is transmitted wirelessly over a Virtual Communication Bus (VCB) for distributed storage and processing by a central Aircraft Health Management Computer (AHMC/NM), which also serves as the Network Manager (NM).

Virtual Communication Bus (VCB): The VCB facilitates communication among sensor clusters, data managers, and AHMCs/NMs for efficient information exchange. It serves as an abstraction of the interconnections between components within all subsystems of a cluster. The VCB operates at two levels:

- Intra-Cluster VCB: This level manages communication between various data managers within the same zonal cluster.
- Inter-Cluster VCB: This level handles communication between different zonal clusters, vehicle health management computers, and distributed data storage. It forms the backbone of the communication framework discussed in Chapter 7.2.

The VCB consist of four layers as shown in the Figure 7.4.

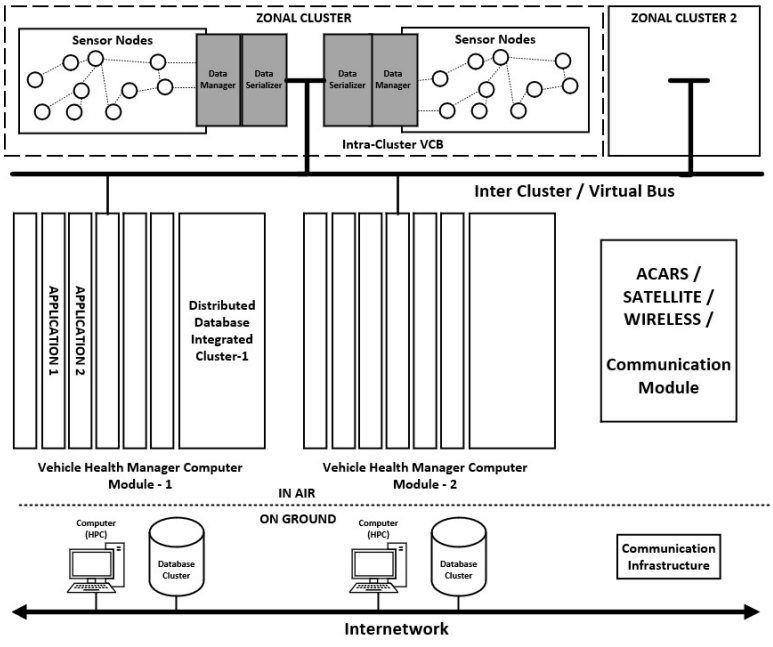


Figure 7.3: Architectural Framework of an IAHM System

The **Hardware Layer** lies at the core of IAHM data communication, comprising the subsystem hardware. The Driver Layer includes the driver soft-

ware responsible for interfacing with the underlying subsystem hardware. The Hardware Abstraction Layer serves as a critical component, enabling the VCB to function as a technology-agnostic interface. By directly interacting with hardware drivers, it provides a standardized, generic interface (abstraction) for the **Application Layer**.

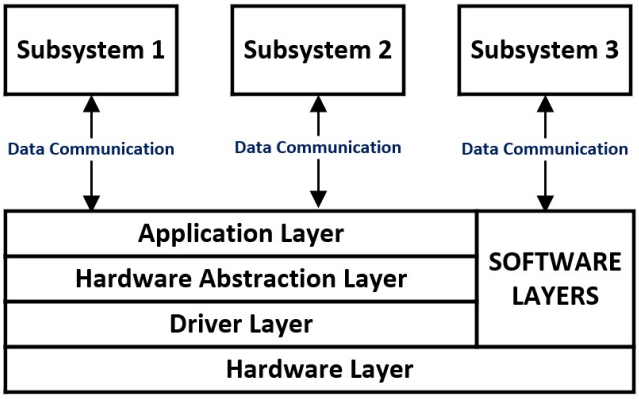


Figure 7.4: Virtual Communication Bus

The **Application Layer** contains generic routines that encapsulate the functionality of the underlying driver layer. Any application developed within the VCB environment operates as part of this layer. It comprises software components and libraries that enable seamless communication between different subsystems. These components both provide services to and receive services from various subsystems, ensuring interoperability. The Application Layer is designed to be reusable across different subsystems, eliminating the need for repetitive development efforts. Additionally, intra-cluster VCBs within this layer are equipped with data serializers, which transform data structures and objects into serialized data streams. This serialization facilitates direct storage in memory devices and ensures efficient data transmission over the network.

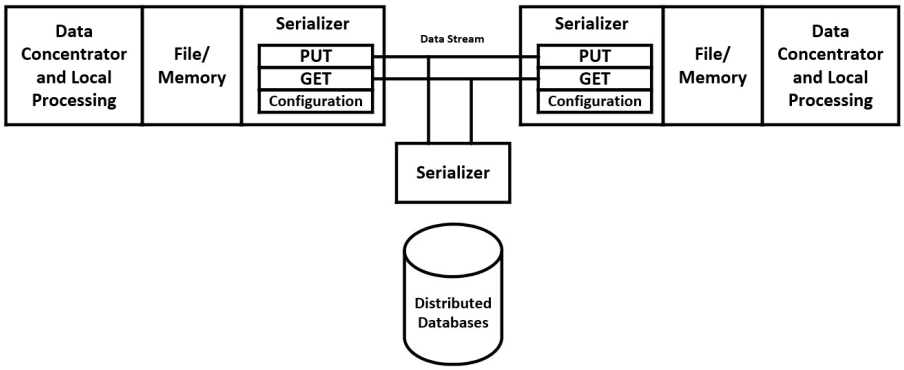


Figure 7.5: Data Serialization and De-Serialization.

The serializers are developed using a hardware-software co-design methodology. In this approach, data objects and structures are serialized into a configurable stream, which can be defined using XML or a custom schema Figure 7.5. Details on VCB and its components are presented in the paper [14].

Aircraft Health Management Computer: AHMC serves as the core computing platform for the onboard IAHM system. It offers the ability to host multiple applications within a virtual environment, effectively separating them. The network manager, which is a crucial component of the IAWSN architecture, is an integral part of AHMC. In addition, AHMC enables inter-process data exchange and incorporates both temporal and spatial partitioning features. It includes its own integrated databases along with modular processing cards that support various health management applications. These modular cards are designed for easy plug-and-play integration and are activated in the AHMC only when their services are required by the vehicle. AHMC processes the acquired data to facilitate decision-making and provide advisories.

Clustered Architecture for Data Processing: IAHM requires data processing and integration between subsystems and systems that need to share information with one another. This collaboration is essential for establishing correlations and making decisions regarding faults and failures. The process involves combining data from two or more subsystems, which aids in identifying the causes of failures and enhances health monitoring. This integration is achieved through a clustered architecture, as illustrated in Figure 7.6. In this architecture, subsystems 1, 2, and 3 communicate and utilize each other's data. When the data from multiple subsystems within a cluster is effectively correlated or integrated, it leads to improved estimates and timely assessments of the health of both the subsystems and the entire cluster. A cluster facilitates communication among its subsystems through a VCB. This setup allows the cluster to be modeled as a composition of interconnected subsystems that in-

teract via a common communication channel. The cluster node, or Zonal Data Concentrator, is capable of sorting and processing or fusing only a defined set of components. The specific data that needs to be fused is configurable in the data manager software. The processed or fused data is then transmitted over the Inter-Cluster VCB.

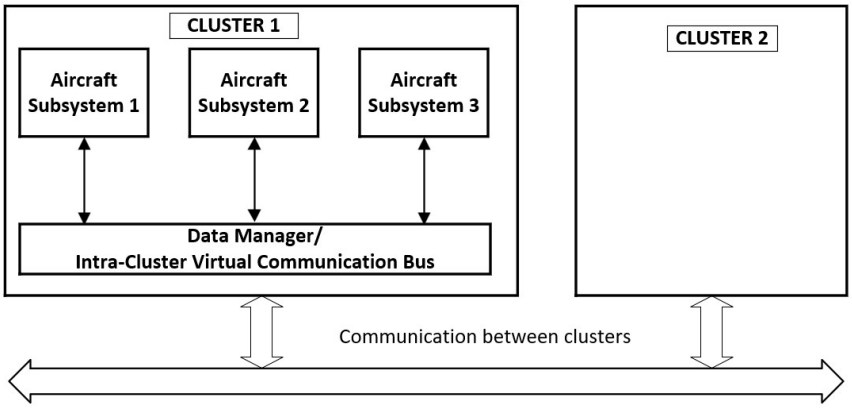


Figure 7.6: Clustered Architecture

Data from different subsystems is converted to similar units before being fused. This conversion is managed at the edge computing level by data managers within the same cluster and by VHMCs for inter-cluster processing.

To perform effective prognostics, the patterns of data observed in different clusters must be stored for future pattern matching with any incoming data. These stored patterns are kept in the AHMC, as shown in Figure 7.3: Architectural Framework of an IAHM system. If no matching pattern is found, pattern recognition algorithms, also stored in the Aircraft Health Management Computers, are activated. It is important to note that the pattern matching and recognition algorithms operate on clusters rather than on individual subsystems. This approach offers several advantages:

- The approach prevents redundant data processing because the interdependent systems are organized into defined clusters. As a result, the pattern matching and recognition algorithms operate on data that is fused within a cluster.
- This organization allows diagnostics to be conducted more effectively, as the cause of a particular data or failure pattern is directly linked to a specific cluster. This enables a comprehensive assessment of the failure's impact on all related subsystems.

By evaluating the pattern across these interconnected subsystems, the risk of failure propagation—which might occur if pattern matching and recognition

were done on individual subsystems—is significantly reduced. This is because identifying and addressing the root cause becomes much easier.

On Ground Data Management: The on-ground system receives health data through various communication channels, as illustrated in Figure 7.3. Once the data is collected, it is stored in a clustered database with a distributed file system. A ground-based AHMC, equipped with capabilities for prognostics and diagnostics, consists of a set of clustered computers that facilitate real-time management, parallel computing, and scalability. This system operates in a cloud computing environment with big data handling capabilities. It performs real-time query processing and prioritizes data effectively. The on-ground station hosts and runs algorithms related to artificial intelligence, machine learning, statistical methods, and decision trees for prognostics and diagnostics. The front end features a dashboard that presents the overall health status of the aircraft, including its systems and subsystems, organized by the zones in which they are located. Additionally, it displays performance metrics, such as the mean time between failures and time to failure for individual systems and subsystems. Further details on On-Ground Data Management and its components are presented in the paper [14].

7.2.3 Structural Health Monitoring

- SHM is a prominent use case for implementing advanced sensor architecture, as it requires a substantial number of sensors and a high data rate for monitoring and detecting structural damage. In the context of aircraft, the structure is equipped with various sensors, including strain gauges, piezoelectric sensors, and fiber optics to mention a few. For this application, we have chosen piezoelectric sensors as the primary devices for structural health monitoring, alongside essential components for signal conditioning, data acquisition, processing, and monitoring, utilizing electronic systems.

In the SHM framework, a cluster comprises an array of sensors embedded in the surface of the aircraft body. These sensor arrays shown in Figure 7.7, form part of sensor nodes, which also include a controller, an analog-to-digital converter (ADC), and a digital-to-analog converter (DAC) for excitation, signal conditioning, and data acquisition. The sensor nodes are designed to be self-sufficient in terms of power management. The controller excites the piezoelectric sensors and gathers digital data from the ADC connected to the sensor arrays.

The data manager is responsible for collecting data from various sensor nodes and performing edge computing to filter useful information from the data bursts. If the change in data is minimal and remains within the predefined threshold, it indicates no structural changes, and the data manager prevents this information from being stored for analysis. In such cases, the data is only sent for storage after an extended period, which helps conserve power. However, if there is a noticeable change in the data or if it signifies an event occurrence, the data manager assigns higher priority to this data, which is then immediately sent for processing to the AHMC)

The filtering and edge computing performed by the data managers are configurable, enabling adjustments based on specific monitoring needs. The AHMC processes the incoming data from different sensor arrays concurrently and conducts analytics to assess the impact on the aircraft's structure, ultimately generating advisory information.

AHMC systems are capable of processing data from various sensor clusters and subsystems. They can perform parallel data processing and share information efficiently. For example, if the AHMC is alerted to or detects a hard landing, it can initiate related applications to request additional information from the sensor array of SHM sensor nodes and data managers. This is accomplished by sending specific data queries. The data manager nodes and the AHMC that hold the data respond with the requested information. Once the data arrives, it is processed in relation to the event, and a report is generated.

The sensor nodes communicate with each other using an Intra-Cluster VCB. The data generated within a cluster is transmitted over a wireless link to an Inter-Cluster VCB, as illustrated in Figure 7.3. Communication at the sensor cluster level—specifically for data transfer between subsystems—minimizes network turnaround time and latency, thereby optimizing throughput.

7.3 IAWSN Architecture for Wireless Power Transfer

Wireless power transfer (WPT) techniques and wirelessly powered devices have already become part of our lives in both commercial and industrial sectors. Examples include wireless charging tables and charging pads in consumer electronics, wireless chargers and charging stations for electric vehicles in the automotive industry [109], and wireless charging for medical implants, such as pacemakers, in the healthcare field [110]. Now, WPT is also making its way into aerospace applications, such as remote charging of UAVs (drones) and exploring methods for power transfer within aircraft.

As we strive to develop more electric and intelligent systems, the IAWSN is being considered for implementation on board aircraft. Wireless communication inside aircraft plays a crucial role in powering architectural elements, enabling a scale-up from the few thousand sensors currently onboard to tens of thousands needed for IAHM applications. In previous chapters, we have outlined the required architecture, network protocols, and security algorithms necessary for deploying the IAWSN.

In this research, we have investigated the feasibility of adopting the IAWSN architecture for WPT to charge sensors and avionics systems on board aircraft. Currently, sensor nodes within the IAWSN architecture receive 28V DC power through wired power lines from the aircraft's DC bus. However, the wireless communication layer of the IAWSN, which allows sensor clusters and nodes to communicate with data managers, could potentially be utilized for wirelessly powering the sensors and associated network elements.

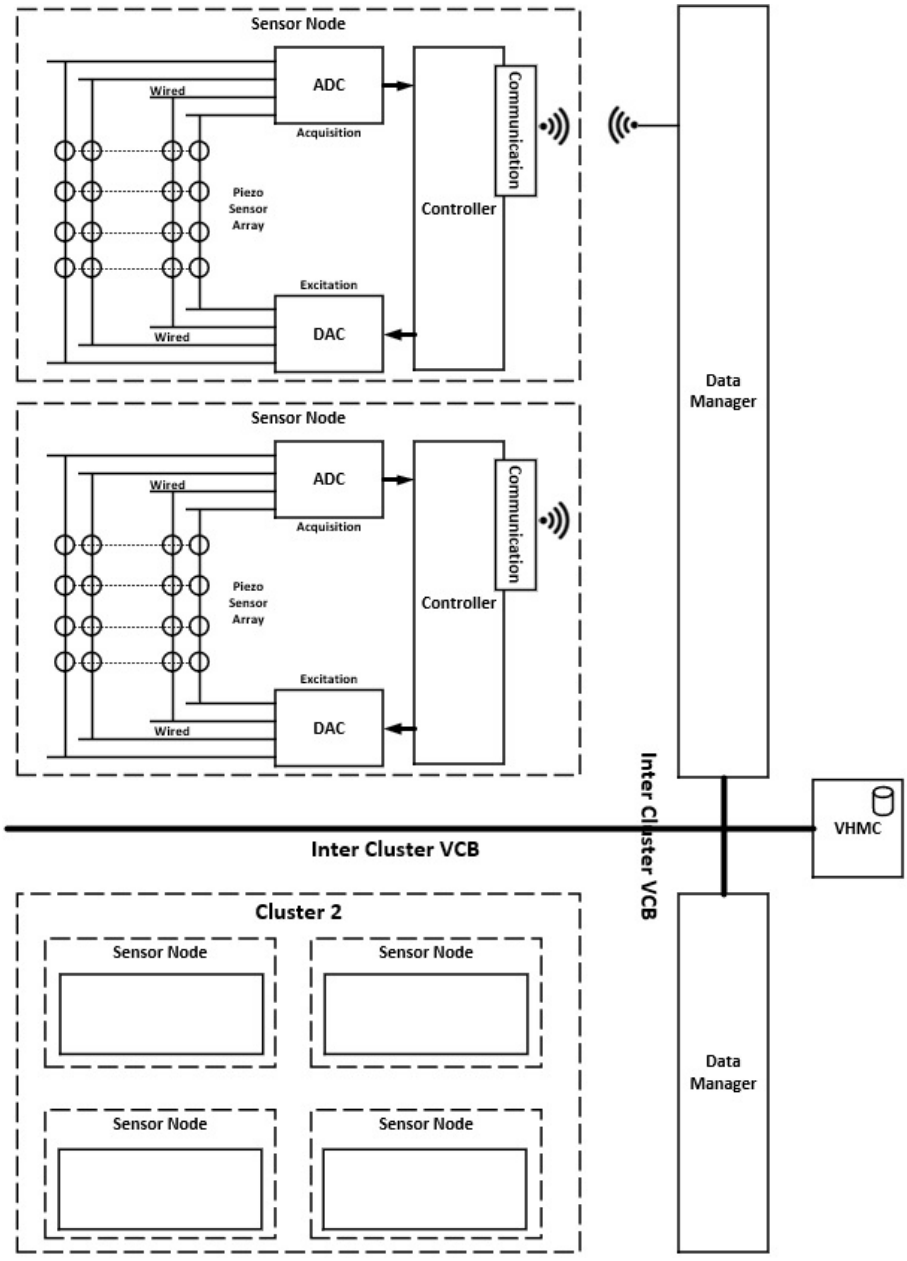


Figure 7.7: Sensor Array Communication with Data Manager

The sensor nodes could be equipped with photovoltaic arrays to harness power through WPT. As illustrated in Figure 7.20, the 28V DC power from the aircraft's DC bus can be converted to laser energy and transmitted to the photovoltaic arrays positioned near the sensor nodes. [15]. Thus, power is transmitted wirelessly using laser power transfer (LPT) techniques to the receiver arrays at the sensor nodes distributed throughout the aircraft. The received power is then used to power the sensors and electronics.

7.3.1 Aircraft Electrical Power System Architecture

The Electrical Power System is crucial for an aircraft, as most systems require electrical power. This includes avionics, flight controls, actuators, communication systems, navigation, environmental controls, and more. As we move towards a More Electric Aircraft (MEA) architecture, the demand for electrical loads is expected to increase significantly.

Electrical power is distributed to various systems within an aircraft through a wire harness that runs throughout the structure. In a typical commercial airplane, this harness can span approximately 100 miles (160 km). Such extensive wiring presents major challenges in terms of scalability and adaptability, especially when introducing additional sensors or network elements. Some of the key challenges include:

1. The installation of wire harnesses is highly cumbersome.
2. The associated costs are significant.
3. Locating faults and conducting maintenance can be tedious.

To address these challenges, Wireless Power Transfer (WPT) techniques have been proposed. In our research, we have explored alternative WPT concepts, with a particular focus on the Laser Power Transfer (LPT) method. We have provided a detailed analysis of the sub-systems involved in LPT, including regulators, light-emitting diodes (LEDs), photovoltaic systems, and light control systems. Additionally, we have presented models of these sub-systems along with simulation results.

We have also discussed the strategies for deploying these systems over Integrated Aircraft Wireless Sensor Networks (IAWSN). For future studies, we have proposed the need for performance assessments focusing on scalability, reliability, and robustness.

In this section, we have examined the existing methods of power generation and distribution in a typical aircraft. Traditionally, power distribution occurs through physical wire harnesses that connect power sources to loads. A typical Electric Power System in an aircraft comprises both AC and DC buses Figure 7.8. The AC bus is supplied by generators connected to the main engines or auxiliary power units (APUs). This AC power is typically either 115V or 230V, operating at 3-phase, 400Hz configuration. The DC bus is powered by rectified

AC from the AC bus, utilizing a Transformer Rectifier Unit (TRU). Additionally, power is supplied to the DC bus through batteries and ram air turbines.

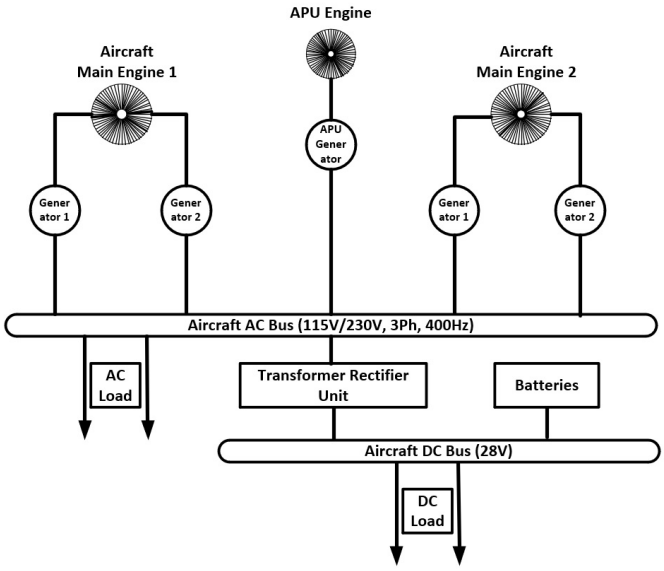


Figure 7.8: Architecture of Aircraft Electrical Power System

Figure 7.8 illustrates a representative architecture of the aircraft power system. The number of generators connected to the main engine and/or Auxiliary Power Unit (APU) depends on the specific power requirements of the aircraft.

Utilization equipment can be classified into two types: AC and DC loads. Based on the criticality of the aircraft equipment being powered, the loads are further categorized into essential and non-essential types. Essential loads are those critical for the safe operation of the aircraft and are supplied by the essential bus, while non-essential loads pertain to systems not directly related to flying the aircraft.

Power from the generation system is distributed to various electrical utilization equipment located throughout the aircraft. A comparison between the conventional electrical system architecture and the More Electric Architecture is discussed below:

Traditional Electric Power System in Aircraft

1. One generator on each of the two main engines.
2. One generator connected to the APU.
3. Power feeders run from generators to EE bay.

More Electric Aircraft

1. Two generators on each main engine.
2. generators connected to the APU.
3. Power feeders run through out the aircraft to supply loads.

The Boeing 787 is a more electric aircraft. The conventional hydraulic and pneumatic loads are converted to electrical loads in the 787 aircraft [111]. To distribute the power, more harness is required. Installation of these harness is complex while it is very difficult to identify fault if any and locate the same. Even though the conventional wire-based power distribution, is reliable, it has dis-advantages in terms of scalability, flexibility and configurability. In addition, it adds up to weight of the aircraft which in turn increases the fuel and operational costs.

7.3.2 Wireless Power Transfer Schemes

WPT is the process by which electrical energy is supplied from a power source to a load, without the use of conventional interconnecting wires. Due to recent improvements in the Electrical Technology the WPT is being deployed in many commercial applications including battery charging, automotive, medical and so on. In the following sections, feasibility of various WPT methods for aircraft applications are analyzed and a case study of WPT is presented. WPT Techniques [92] are broadly classified into 5 types namely:

1. Inductive
2. Capacitive
3. Laser
4. Radio Frequency and
5. Acoustic

Inductive Power Transfer: In inductive coupling or inductive power transfer (IPT), power is transferred between coils of wire by a magnetic field, Figure 7.9. Inductive coupling is the oldest and most widely used wireless power technology, and virtually the only one so far which is used in commercial products.

Capacitive Power Transfer: Capacitive Power Transfer (CPT) referred as electric coupling, makes use of electric fields for the transmission of power between two electrodes (an anode and cathode) forming a capacitance for the transfer of power, Figure 7.10. The capacitive coupling has only been used practically in a few low-power applications because of very high voltage requirements to transmit significant power and can be hazardous since it can cause unpleasant side effects such as noxious ozone production.

Inductive and Capacitive wireless power systems, the transmitters and receivers are to be placed near each other. The coupling factor between transmitters and receivers depends on several design parameters and largely determines the link efficiency. The transmission range of Inductive and capacitive wireless power systems is only a few centimeters, which makes it not feasible for WPT for IAWSN applications.

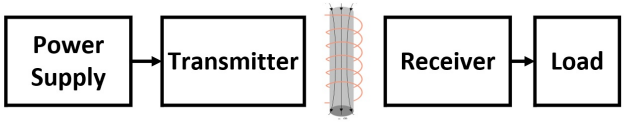


Figure 7.9: Inductive Power Transfer System

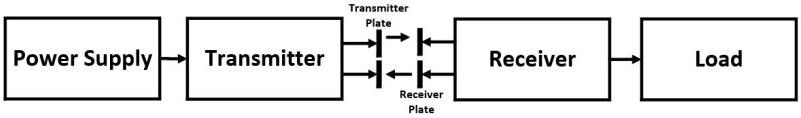


Figure 7.10: Capacitive Power Transfer System

Radio Frequency Power Transfer: A radio frequency (RF) wireless power system can convert electromagnetic energy into a usable direct current (DC) voltage. The key components of an RF wireless power system are the antenna and the rectifier circuit, which enable the conversion of RF power or alternating current (AC) into DC energy, as illustrated in Figure 7.11.

RF power can be harvested from both ambient and dedicated sources. Ambient RF sources, such as Wi-Fi or cellular systems, typically have a very low power density available to energy harvesting nodes. At a large scale, the frequency bands with the highest power density can vary, which complicates the design of a single, optimal energy harvesting circuit. To achieve higher power levels, dedicated RF sources are often used.

In practice, within aircraft, RF power levels are often limited by regulations and safety standards [7]. However, the main advantages of RF wireless power transfer (WPT) include the ability to direct power to the receiver, thereby increasing overall efficiency, and having a more predictable energy supply at the nodes. Nonetheless, multiple frequency bands may be necessary to increase the harvested power.

For aircraft applications, RF WPT can effectively power devices that require DC power. Using a dedicated RF source is essential to enhance conversion

efficiency and ensure a reliable energy supply. However, RF power transfer may encounter challenges, particularly in terms of interference with existing safety-critical aircraft systems [7]. Addressing these interference issues is crucial for the practical implementation of RF wireless power transfer solutions.

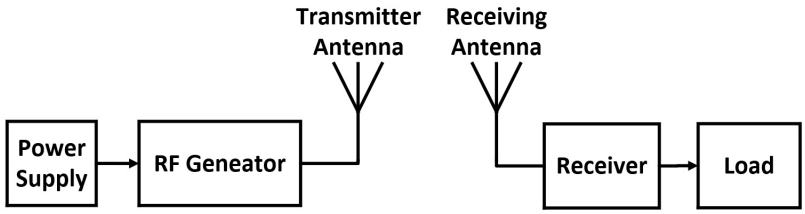


Figure 7.11: Radio Frequency Power Transfer System

Laser Power Transfer: LPT can provide a few mWs to even several kWs of power to a device. Typically, high intensity laser power beam (HILPB) systems are used, since these LPT techniques are mainly applied for relatively high-power applications (up to several kilowatts).

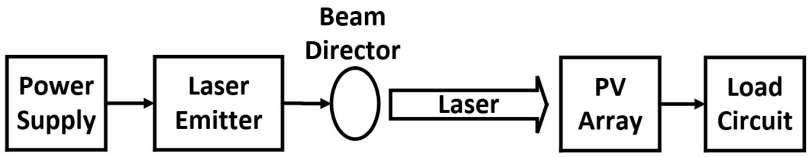


Figure 7.12: Laser Power Transfer System

However, in this chapter, we have focused on gradual progression from low power to medium and then to high power. An HILPB, transmitter system consists of a laser emitter, followed by beam shaping with a set of optics, after which the beam is directed to the remote Photo Voltaic (PV) array. The beam director is an important element since the alignment in an LPT setup determines its actual transfer. At the receiver, the PV array converts the laser light back into electricity, based on the photoelectric effect. It is important for efficiency to have a good match in terms of used wavelength and beam intensity between the laser and PV element. For Aircraft WPT, laser wireless power transfer can be used to power devices which use DC power. dedicated laser source is required for increasing the efficiency of conversion and have more predictable energy supply.

Acoustic Power Transfer (APT): In acoustic power transfer, acoustic waves are used as carriers to convey energy. A typical structure of an APT system is

WPT Technology	Acronyms	Power Transfer Range	Transmission Range	Efficiency
Inductive	IPT	W to MW	cm	High
Capacitive	CPT	W to MW	mm / cm	High
Laser	LPT	W/KW	m/km	Medium
Radio Frequency	RFPT	mW/KW	m/km	Low
Acoustic	APT	mW/KW	m/km	Medium

Table 7.1: Wireless Power Transfer Technologies

shown in the Figure 7.13. APT consists of acoustic transducers at the transmitting end, electrical energy is converted into vibrations, which in turn result in pressure waves radiating throughout the medium. The propagated pressure waves are then collected by a receiving transducer and converted back into electrical power. Rectifier ensures a stable DC voltage, which can be used to drive a load or charge an energy buffer (e.g., battery).

Figure 7.13: Acoustic Power Transfer System

Use Case: Wireless Power Transfer - In aerospace, WPT is most suitable for supplying power to devices placed in the remote locations, where accessibility of the Line Replaceable Units is challenging. Hence the coverage needs to be in the order of at least few meters. For example, the sensors such as Fuel sensors, Engine sensors, Air Data Sensors, Fire protection system, etc. which are placed in the remote locations and supplied by a harness which runs through harsh environments and in case of any failure, accessing and fixing the harness is challenging.

Technology Selection and Challenges: In this research the applicability of above mentioned WPT techniques as listed in the Table, 7.1 are analyzed for an aircraft configuration.

The transmission range of the IPT and CPT are in the order of mm/cm. Even though the efficiency is higher, they are not suitable for long-distance applications. In aircraft applications, the power transfer required is in the order of tens of meters. Typically, less than 50 meters with options for extenders for increased range inside the aircraft (maximum length of 100 meters). The IPT and CPT are not suitable. The other WPT methodologies have been analyzed for medium to long-distance power transfer in an aircraft. The electromagnetic uncoupled technologies, including Laser, RF, and Acoustic, are found suitable

for medium to long distance power transfer in an aircraft. However, RF and Acoustic may impact the safety critical systems installed in the vicinity due to EMI/EMC interferences generated by the RPT and APT. Hence these techniques are not considered for power transfer in aircraft. Due to the distance coverage and considering no impact on the environment, the LPT technique has been selected for the use case under consideration. For LPT, the expected efficiency range varies from 10% to 40% with design optimization [92]. In this research, the feasibility for low power (28V, 2Amps) applications is being verified.

Laser Power Transfer: The LPT system consists of three main sub-systems:

1. Laser emitter
2. Photovoltaic array
3. LED Current controller

A functional block diagram of a typical LPT from aircraft DC bus to the utilization equipment is shown in the Figure 7.14. The power from the aircraft DC bus is converted to light energy using the photo electric diodes and then transmitted as a Laser beam to the photovoltaic array placed near the utilization equipment. The emitted light signal wavelength is adjusted by the control circuit based on the feedback from the photovoltaic array. The LED is a current-controlled device, and the intensity of the light generated is directly proportional to the amount of current flow. The V-I characteristics look similar to the diodes Figure 7.15. The breakdown voltage varies for the different materials and color spectrums.

A Laser source of Red or Infrared diode is ideal for WPT as these diodes have higher wavelengths (660-850nm) and better conversion efficiency (50-80%) when compared to other spectrums. The actual color of a light emitting diode is determined based on the wavelength of the light which in turn depends on the semiconductor compound used in the PN junction. The typical semiconducting materials used for various color spectrums are listed in Table 7.2.

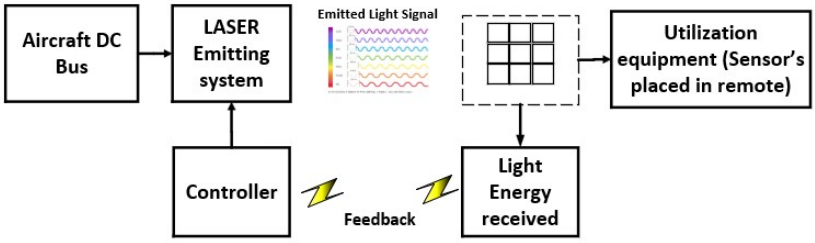


Figure 7.14: Laser Power Transfer System

For the selected wavelength (Red and Infra-red) the Light emitting diodes which are suitable for Laser Wireless Power Transmission are.

- Gallium Arsenide (GaAs) – infra-red

- Gallium Arsenide Phosphide (GaAsP) – red to infrared,orange
- Aluminum Gallium Arsenide Phosphide (AlGaAsP) – high-brightness red, orange-red, orange, and yellow

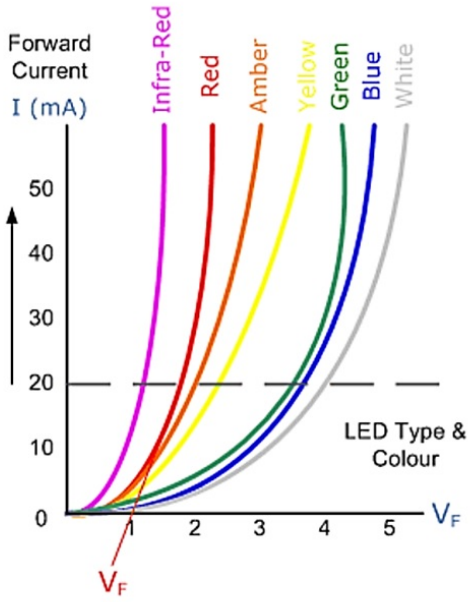


Figure 7.15: Different Types of LED Power Transfer

Controlling light-emitting diodes (LEDs) using driver circuits is crucial for adjusting the intensity of the emitted light, which in turn impacts the power transfer and overall efficiency of the system.

The literature discusses various LED driver circuits, including linear and switching power supplies. While straightforward, linear current regulators have disadvantages such as low efficiency and bulky size. On the other hand, switching mode LED drivers, which typically feature a higher-order filter, are common for generating current with low ripple. However, these systems can also be heavy, bulky, and have limited dynamic response.

To address the issue of dynamic response, this research utilizes a bridge-type LED current regulator.

Also, from the literature it is found that the Light Diode operating in pulse mode by using a driver circuit provides higher efficiency and performance [88]. In this research, a bridge type current regulator-based drive circuit is used for driving the Light diodes Figure 7.16.

Color	Wavelength (nm)	Vf @ 20mA	Semiconductor Material
Infra-Red	850 - 940	1.2 V	GaAs
Red	630 - 660	1.8 V	GaAsP
Amber	605 - 620	2.0 V	GaAsP
Yellow	585 - 595	2.2 V	GaAsPN
Green	550 - 570	3.5 V	AlGaO
Blue	530 - 505	3.6 V	SiC
White	450	4.0 V	GaLnN

Table 7.2: LED Characteristics

This is an active ripple filter-based driver to overcome the ripples. The 28V delivered from the aircraft DC bus is stepped down using a Buck converter and applied to the LED's. The Light emitting diode intensity is controlled using the current regulator circuit. The current regulator is controlled to obtain optimum light intensity, power at the utilization equipment, and efficiency. The light generated is pointed to the photovoltaic array placed near the utilization equipment.

Photovoltaic Array: There are four different configurations of photovoltaic array, namely Series, Parallel, Cross-Tied (CT) and Bridge configuration as shown in the Figure 7.17.

A study has been conducted to analyze various Laser power transfer control methodologies. Various subsystems of Laser Power Transfer including buck converter, LED drive control, photovoltaic array and utilization equipment loads were modeled, simulated and presented in Figures 7.18 and 7.19. The proposed H-bridge based current control circuit has been modeled and the performance has been simulated.

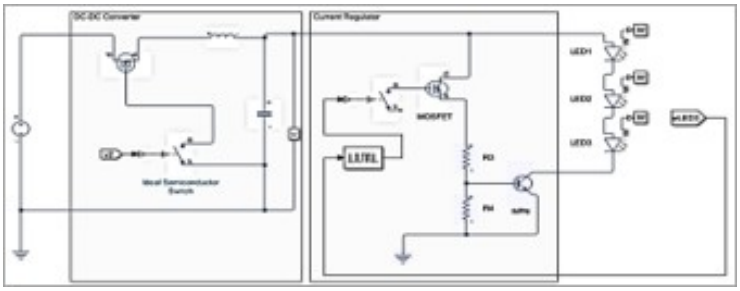


Figure 7.16: LPT - LED Drive Circuit

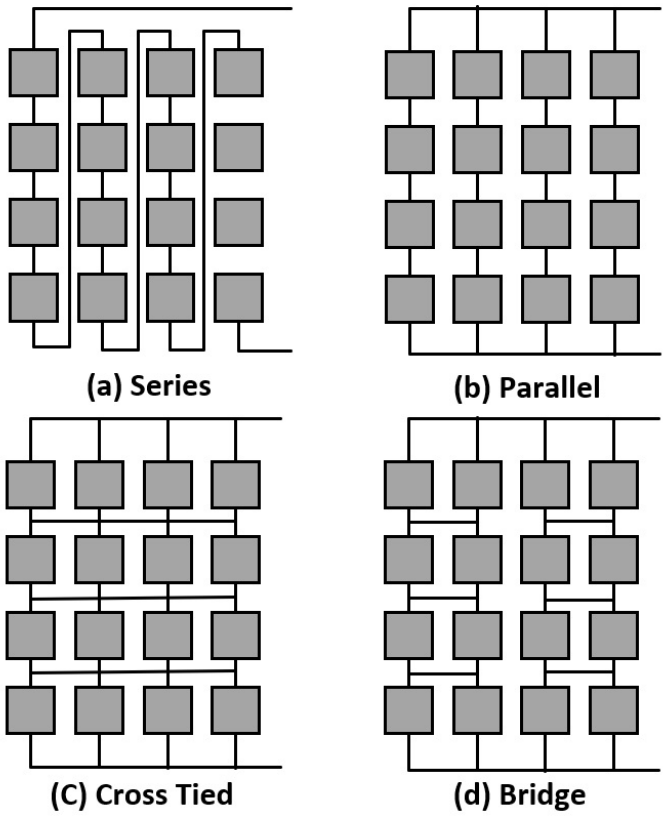


Figure 7.17: Photovoltaic array Configuration (a) Series (b) Parallel (c) Cross Tied and (d) Bridge

The current controller based on the power and intensity requirement at the load end has been achieved.

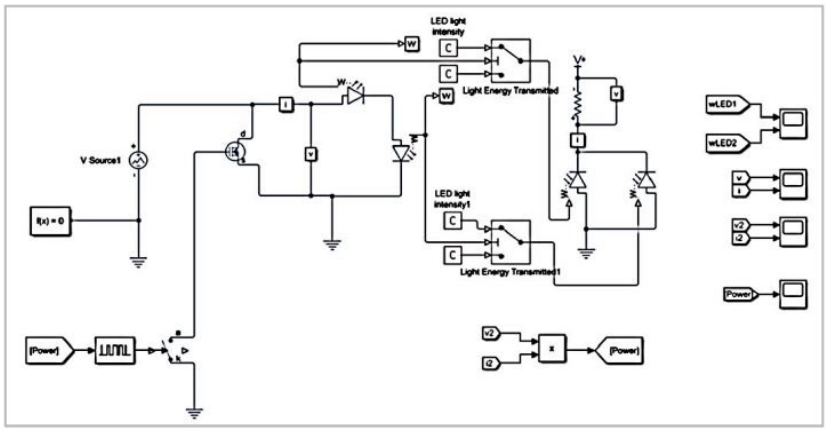


Figure 7.18: Laser Power Transfer System

Performance Analysis of the Control System: The output power control based on the LED current control is depicted in Figure 7.19. The intensity of the independent row of photovoltaic array is adjusted in such a fashion to ensure continuous power to the load. At any given point in time, one row of LED is turned ON so that the corresponding row of the photovoltaic array receives the power. The time delay between the switching of each row corresponding to the wavelength of the Infra-red rays make the system optimum for power transfer.

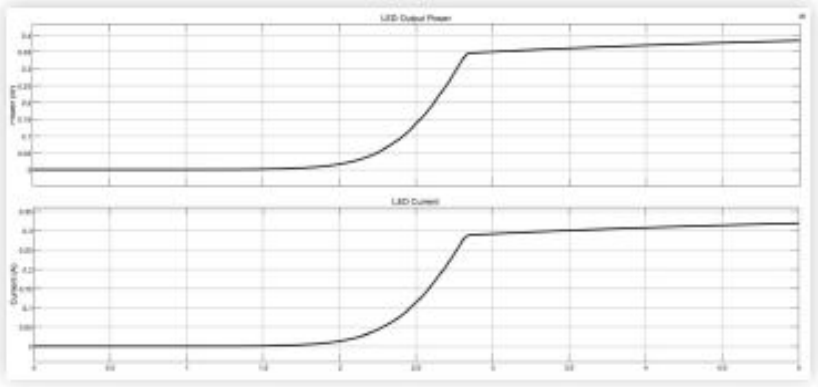


Figure 7.19: LPT Closed Loop Control

Performance of LPT: Based on the analysis we find that the Laser Power transfer is suitable for low power DC system which are placed in remote locations of the aircraft. Since the Optical Wireless Power Transfer (OWPT) needs a separate medium which is similar to the wire harness and needs to be installed in the aircraft, the OWPT may not be suitable for harsh environments.

Implementation Strategy: In the previous chapters of this thesis, we have discussed the architecture of IAWSN for communicating between Avionics components wirelessly. We have also analyzed the feasibility, design requirements and operation of Laser based WPT. In this section we present a proposal to wirelessly power the sensors and network elements using LPT technique and extend the IAWSN architecture to include WPT elements as shown in the Figure 7.20.

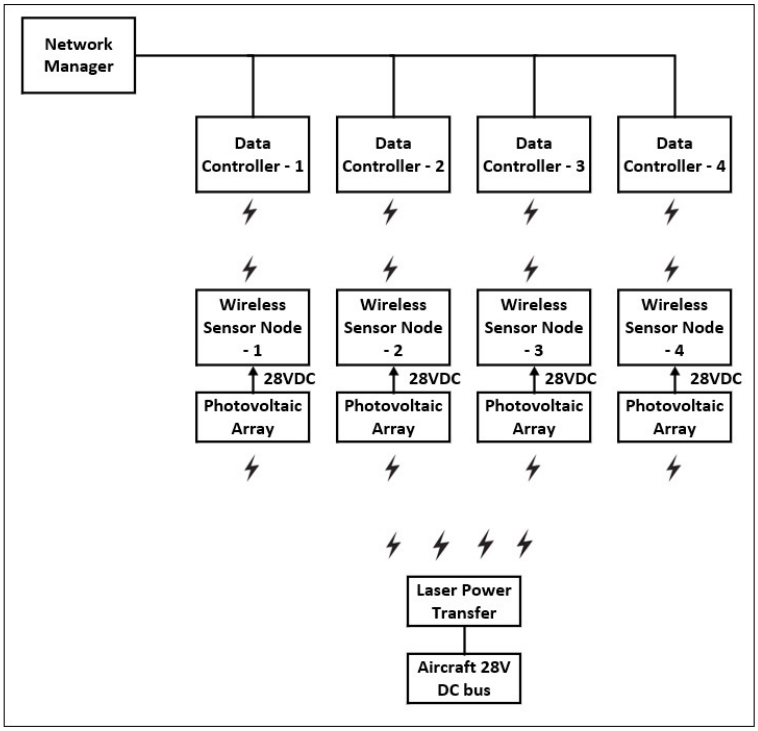


Figure 7.20: IAWSN Architecture for LPT System

We propose to deploy the WPT for the sensor nodes placed in the remote locations as part of the IAWSN and futuristic WAIC architecture. We have discussed the key factors influencing the proposal.

Avionics Communication Bus: Avionics bus is using Local area networks on most platforms, based on the standards, specific to aerospace industry like ARINC 429, AFDX (ARINC 664), MIL-STD 1553, CAN, etc. However, wired communication poses constraints on scalability and adaptability for the introduction of any additional sensor onboard aircraft. The addition of any sensor calls for modification of wire harnesses and re-certification. The industry is exploring wireless power transfer for IoT type of applications using WAIC/I-

AWSN architecture [112] and [113].

IAWSN / WAIC network allows overcoming the above-said constraints and allows a scalable architecture for IAHM applications. Wireless network inside aircraft is being developed using WAIC standards at 4.2 GHz and can be interfaced with cellular network, SATCOM, ADS-B, and terrestrial network outside aircraft communications. The network manager and associated interface components can connect data from sensors and other LRUs to the data manager and can further interface with outside aircraft as a Gateway device. Wireless communication inside aircraft plays a key role in powering the architecture to scale from a few hundred sensors currently onboard aircraft to tens of thousands of sensors needed for IAHM applications.

The wireless network architecture IAWSN has been discussed in detail in chapter 3, Figures 3.9 and 6.1.

As shown in Figure 7.20, Nodes communicate with data managers on wireless links whereas network manager communicates with the data managers over wired medium. The wireless sensor network inside an aircraft needs to be scalable and configurable mainly with respect to the nodes. This is because there is likelihood that the nodes in terms of sensors and avionics may be increased both in number and variety. Data managers once installed may not be replaced before a failure or expiry of their lifetime.

The sensor nodes in the current WAIC architecture are being supplied by 28V DC power from aircraft DC bus through wired power lines. A wireless power transfer system makes the WAIC network fully wireless. Referring to Figure 7.20, The 28V DC power from aircraft DC bus is converted to laser energy and transmitted to the photovoltaic array placed near the sensor nodes. Thus, power is transmitted wirelessly using the LPT technique to the receiver arrays at the sensor nodes distributed across the aircraft. The received power is used to power the sensors and electronics. However, optimum location of LPT systems has to be studied for optimum performance while maintaining the safety of assets and human being involved in aviation.

7.4 Chapter Summary

In this chapter we have presented two applications of IAWSN architecture scalable to WAIC:

1. A qualitative analysis of existing health monitoring architecture and presented a scheme for adopting IAWSN architecture for IAHM application.

2. A trade study of wireless power transfer schemes and a proposal to adopt IAWSN / WAIC architecture for WPT inside aircraft

We have presented an integrated architecture consisting of data acquisition, data processing, and data fusion, with capabilities to perform diagnostics, prognostics, and decision-making. We have also presented a clustered architecture

as part of the presented framework. This feature enables effective data collection for diagnostics and prognostics with faster localization of failures/faults.

We have proposed that the implementation of the IAHM architectural framework needs to consider the strategies for integrating the capabilities into existing systems and retrofitting. The implementation strategy should include testability and maintainability to ensure retrofit, testability and verifiability as needed. The integrated approach of IAHM requires special considerations for system safety assessment and failure hazard analysis to arrive at the required design assurance levels [93] of different partitions of the IAHM system.

System requirements for safety analysis and failure mode analysis are to be apportioned to address high criticality applications from low criticality applications at both hardware and software level and allow communication through very well defined and safe access interfaces. The interfaces are developed at highest level of criticality of applications requiring data exchange while the applications themselves are developed at their determined level of design assurance based on their impact on safety of aircraft.

In this chapter, the importance of accelerating research in the WPT in aircraft is analyzed, alternate technologies are verified for feasibility and performance. Based on the study, the LPT is proposed for 28V DC low power applications, especially LRU's placed in locations where the harness installation and maintenance are challenging. For the proposed system, a unique control system to control the emission characteristics of Laser transmitters has been designed, modeled and simulated to demonstrate the LPT. Advancements in Electric Aircraft, Intelligent systems and Wireless Aircraft inside communication strategies could be supporting aspects for deployment of WPT. The technology described in this chapter can be demonstrated using COTS hardware. Adopting this technology in any given platform will have positive impact by increasing flexibility, scalability, sustainability by possible reduction in weight of the system in addition to reduction of carbon emissions. Advancements in this technology accelerates design and deployment in various aviation platforms like aircraft, UAV's, UAM's and drones.

Chapter 8

Conclusion and Future Work

8.1 Summary of Contribution

Architecture of IAWSN

1. We have introduced a layered hierarchical network architecture in which sensor clusters communicate wirelessly with data managers, while the data managers connect to the network manager through wired links. To ensure fault tolerance against potential software and hardware failures in the network components, we have implemented two levels of redundancy: spatial and spectral. The network algorithms guarantee seamless connectivity between sensor clusters and data managers. In the event of a fault, sensor clusters can smoothly switch to an alternate frequency spectrum or data manager, depending on the issue encountered.

2. We have developed and studied a priority queuing model that considers variations in the priority of sensor data during different phases of flight operations. This model is based on the requirements of the network, and we have analyzed the traffic distributions related to the frequency of data transmitted by various sensors into the communication network at each phase. Both preemptive and non-preemptive policies are used in the development of the model to conduct a stochastic analysis of different Quality of Service (QoS) parameters relevant to evaluating the network's response to dynamic traffic characteristics. The findings indicate that the non-preemptive policy is more effective than the preemptive policy in optimizing the system's response to data flow in a typical Intra Aircraft Wireless Sensor Network (IAWSN).

3. A communication scheme based on Code Division Multiple Access (CDMA) has been designed and simulated for devices operating under the IEEE 802.15.4 protocol. This scheme aims to improve devices' resistance to high-power interference from Wi-Fi devices. By implementing CDMA in IAWSN, which function according to both the IEEE 802.15.4 and IEEE

802.11 (Wi-Fi) standards on aircraft, we have addressed the interference issue that reduces Quality of Service (QoS). The results demonstrate significant improvements in the overall performance of IAWSN.

Security framework for IAWSN

This research presents a comprehensive security solution for Wireless Sensor Networks (WSN) that is scalable for Wireless Avionics Intra-Communications (WAIC) and is the first of its kind in the existing literature. The major contributions of this research are as follows:

1. We have introduced an optimized security architecture featuring a group-based key management scheme and a dynamic symmetric key cryptography algorithm.
2. We have conducted an empirical evaluation of network security by analyzing the resilience of the connection between any two sensor nodes in the event of node capture due to adversarial attacks.
3. We have proposed a scheme to optimize encryption algorithms, resulting in lightweight computational modules that can operate effectively in resource-constrained environments onboard aircraft.
4. We have conducted a performance analysis of critical elements, focusing on the strength of encryption keys and the effects of computational and network overheads on network throughput.

Applications of IAWSN

We have discussed two applications of the IAWSN architecture that encourage the aviation industry to adopt this technology. These applications aim to enhance aircraft intelligence, connectivity, scalability, and autonomy while ensuring safety, reliability, and availability.

Integrated Aircraft Health Management

1. We have presented a qualitative analysis of existing health monitoring architectures and emphasized the integration of IAWSN into a comprehensive framework that includes data acquisition, processing, and fusion. This integrated architecture is designed to perform diagnostics, prognostics, and decision-making.
2. Additionally, we have introduced a clustered architecture as part of this framework. This feature enhances data collection for diagnostics and prognostics, enabling quicker identification of failures or faults.
3. We presented methods for implementing the discussed architectural framework, necessitating strategies for integrating these capabilities into existing systems and retrofitting them. We also highlighted the importance of testability features to facilitate efficient testing.

IAWSN architecture for Wireless Power Transfer

We have analyzed the feasibility of using the IAWSN architecture for wireless power transfer (WPT) to supply power to sensor clusters distributed throughout the aircraft. We have conducted a trade study of various WPT techniques and selected Laser Power Transfer (LPT) to supply power to sensor clusters located in remote areas such as the wing bay and cargo hold. This approach ensures that LPT does not interfere with operators or crew members. The proposed IAWSN architecture will enable the integration of wireless power capabilities with data applications.

8.2 Conclusion

The requirements for an IAWSN have been thoroughly analyzed, leading to the design and evaluation of a robust IAWSN architecture within a laboratory-simulated aircraft environment. The combination of priority queuing theory and Code Division Multiple Access (CDMA) for an IEEE 802.15.4-based IAWSN has resulted in optimized network throughput throughout all phases of flight.

Furthermore, a comprehensive network security framework employing dynamic symmetric cryptography for key generation and group-based key management techniques has effectively provided robust and efficient network security while meeting performance metrics in the simulated aircraft environment. The IAWSN developed, implemented, and evaluated in this work has been proposed for two significant applications: (1) Integrated Aircraft Health Monitoring (IAHM) and (2) Wireless Power Transfer (WPT). These applications aim to expedite the development of next-generation aircraft platforms, particularly Next Generation Single Aisle platforms, which will incorporate systems such as Pilot Assistance Systems, Pilot Monitoring Systems, and Single Pilot Operations. This progress is expected to lead to the future development of Autonomous Aircraft or Pilotless Transportation. However, the successful implementation of IAHM and WPT necessitates special considerations regarding system safety assessment and failure hazard analysis to determine the required design assurance levels for the various components of the Integrated Aircraft Health Management (IAHM) system. Proper partitioning of requirements based on safety analyses and failure modes is essential to differentiate between high- and low-criticality applications at both the hardware and software levels. This partitioning enables communication through well-defined and secure access interfaces. These interfaces are developed at the highest level of criticality for applications that require data exchange, while the applications themselves are designed according to their specific design assurance levels based on their impact on aircraft safety.

8.3 Future Work

Future research could focus on a detailed analysis of IAWSNs regarding various performance parameters. This includes:

1. Optimal number of network nodes for specific applications, which can be determined by
   (a) Evaluating network performance in adverse conditions such as electromagnetic interference (EMI) and electromagnetic compatibility (EMC),
   (b) Identifying the best locations for network elements, including wireless routers, smart sensors, actuators, and other avionic equipment, and
   (c) Optimizing the placement of the network manager within a defined aircraft configuration to ensure scalability and simplicity of the network.
2. There is a need to develop technologies that support the dynamic configuration of avionic elements like sensors, actuators, controllers, and display elements with varying data types and performance characteristics. This analysis will help evaluate network throughput, scalability, security, and robustness.
3. The proposed architecture can be expanded for a comprehensive Internet of Things (IoT) implementation that will include
   (a) Edge computing nodes for pre-processing sensor data.
   (b) A dynamic or tactical cloud for temporary storage and post-processing.
   (c) Linking of IAWSN to external networks such as SATCOM, cellular networks, and Automatic Dependent Surveillance-Broadcast (ADS-B) through gateway communication managed by the Network Manager.
4. Current research has primarily focused on implementing the physical (PHY) layer of the CDMA scheme for Wireless Sensor Networks (WSNs). Further studies are needed to explore the changes at the Medium Access Control (MAC) layer to fully leverage CDMA capabilities for WSNs and assess the resulting performance metrics. While implementing CDMA for IEEE 802.15.4 radio has mainly been validated through simulations, extending this to physical implementations in real aircraft environments could be beneficial.
5. Research on priority queuing theory and related topics is effective for selecting appropriate MAC protocols that meet WSN specifications. It is also important to consider the number of endpoint systems in the network and the specific characteristics of the chosen MAC protocol to ensure

proper system response. Guaranteed end-to-end delay should be rigorously examined alongside the application of CDMA, as this addresses throughput issues related to coexistence and interoperability in future scenarios.

Advanced Topics: As technology for IAWSN and Wireless Avionics Intra-Communications (WAIC) advances, researchers are identifying various challenges. Ongoing research is focused on enhancing Quality of Service (QoS) by addressing interference and employing artificial intelligence and machine learning (AI/ML) to solve these issues. Key insights include:

1. 6TiSCH-CLX - A framework to address the demanding QoS requirements communication at the network and Medium Access Control (MAC) layers, addressing latency and reliability challenges agnostic of the physical layer. 6TiSCH-CLX is an extension of 6TiSCH [44].

2. Narrow Band-IoT - Long Term Evolution (LTE)/Fifth Generation (5G) wireless technologies for low data rate WAIC applications using analytical models and Narrow-Band Internet of Things (NB-IoT) hardware experiments [45].

3. Impact of 5G on co-existence of RA & WAIC - Interference due to RA - Evaluation of wire-less communications techniques for their feasibility to be employed as WAIC systems ensuring reliable communications in the presence of interference due to radio altimeter systems [46].

4. Analysis of the recently raised concerns [47] on the potential impact of 5G over Radio Altimeter and WAIC, as they operate at the same frequency band.

5. Simulation model of avionics compartment channel and its fading distribution to analyze the maximum system arrival rate for selected average SNR and as per ITU-R guidelines [48].

6. AI for IAWSN - Analysis of several reliability, trust, interoperability and latency issues that must be addressed before WAIC / IAWSN technology becomes commercial. AI is expected to boost this technology's applicability, contributing to realizing the concept of "fly-by-wireless" [50].

These studies collectively address key technical, regulatory, and operational challenges, underscoring the role of emerging technologies in advancing IAWSN and WAIC applications.

Bibliography

[1] P. R. Ramanatt, K. Natarajan, and K. R. Shobha, "Challenges in implementing a wireless avionics network," *Aircraft Engineering and Aerospace Technology*, vol. 92, no. 3, pp. 482–494, 2020.

[2] P. Vadgaonkar, U. Janardhan, and A. Sivaramasastry, "Wireless sensing - future's password to digital avionics system," *SAE Technical Paper*, no. 2014-01-2132, pp. 482–494, 2014.

[3] P. Park and W. Chang, "Performance comparison of industrial wireless networks for wireless avionics intra-communications," *IEEE Communications Letters*, vol. 21, no. 1, pp. 116–119, 2017.

[4] P. Reji, K. Natarajan, and K. R. Shobha, "Performance evaluation of wireless protocols for avionics wireless network," *Journal of Aerospace Information Systems*, vol. 17, no. 3, p. 160–170, 2020.

[5] P. Reji, K. Natarajan, and K. Shobha, "Secured wireless network for aircraft intra communication," in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1–6, 2020.

[6] "Technical characteristics and spectrum requirements of wireless avionics intra-communications systems to support their safe operation," Tech. Rep. M.2283-0 (12/2013), ITU-R, 2013.

[7] "Fcc(14 cfr) part 91, use of portable electronic devices aboard aircraft," Advisory Circular FAA CFR FCC(14 CFR)part 91, 91.21-1D, U.S. Department of Transportation Federal Aviation Administration, FCC, Oct 2017.

[8] "Prohibition on airborne operation of cellular telephones," Advisory Circular FAA CFR FCC(14 CFR)part 91, 91.21-1D, Federal Communications Commission, FCC, Oct 2024.

[9] D. H. KIM, D. S. KIM, J. M. LEE, and S. P. AHN, "Comparative study of wireless network technology for avionic sensor actuator networks industrial wireless communication technology for avionic systems," in *Sixth*

International Conference on Advances in Computing, Control and Networking - ACCN 2017, ACCN, p. 92–96, Institute of Research Engineers and Doctors, feb 2017.

[10] A. Sivaramasastry, P. Ramamurthy, S. Bajekal, and K. Banerjee, "Robust wireless sensor network for intra-aircraft communication," in *Proceedings of the 4th World Engineers Summit*, 2019.

[11] A. Sivaramasastry, S. K. Das, C. Mazumdar, K. Banerjee, and M. S. Barik, "Priority queuing model for analysis of network traffic in flight operations of commercial aircraft," in *2017 International Conference on Circuits, Controls, and Communications (CCUBE)*, pp. 25–30, 2017.

[12] Adishesha, P. Ramamurthy, K. Banerjee, and M. S. Barik, "A cdma based approach for qos improvement in intra-aircraft wireless sensor networks (iawsn)," in *SAE Technical Paper Series*, no. 2024-26-0435, (PA, United States), SAE International, 2024.

[13] A. CS, M. Barik, and K. Banerjee, "A comprehensive security framework for an intra-aircraft wireless sensor network," *IEEE Access*, no. Access-2025-32254, 2025.

[14] A. K. Jha, G. Sahay, and A. Sivaramasastry, "Framework and platform for next generation aircraft health management system," in *SAE Technical Paper Series*, no. 2017-01-2126, (PA, United States), SAE International, 2017.

[15] Adishesha, A. K. Thirunarayana, M. Shreshthi, M. S. Barik, and K. Banerjee, "Wireless power transfer in aircraft systems," in *SAE Technical Paper Series*, no. 2024-01-1927, (PA, United States), SAE International, 2024.

[16] T. Ricker, "Avionics bus technology: Which bus should i get on?," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, vol. 7, p. 1–12, IEEE, sep 2017.

[17] B. Chen, D. Gao, and L. Wang, "Research of multi-information integration for the aircraft ground centralized deicing monitoring system based on wireless data transmission," *IEEE Access*, vol. 6, p. 52460–52470, 2018.

[18] C. Fitzhugh, J. Frolik, R. Ketcham, J. Covell, and T. Meyer, "Multipath fading in airframes at 2.4 ghz," in *The 2005 IEEE Annual Conference Wireless and Micrwave Technology, 2005.*, WAMIC-05, p. 4, IEEE.

[19] C. Heller, C. Blumm, S. Bouckaert, W. Liu, I. Moerman, P. V. Wesemael, S. Pollin, T. Sole, and Z. Padrah, "Spectrum sensing for cognitive wireless applications inside aircraft cabins," in *2012 IEEE/AIAA 31st Digital Avionics Systems Conference (DASC)*, p. 1–19, IEEE, Oct. 2012.

[20] R. Alena, J. Ossenfort, T. Stone, and J. Baldwin, "Wireless space plug-and-play architecture (spa-z)," in *2014 IEEE Aerospace Conference*, p. 1–17, IEEE, Mar. 2014.

[21] T. Stone, R. Alena, J. Baldwin, and P. Wilson, "A viable cots based wireless architecture for spacecraft avionics," in *2012 IEEE Aerospace Conference*, p. 1–11, IEEE, Mar. 2012.

[22] T. Andre, K. Hummel, A. Schoellig, E. Yanmaz, M. Asadpour, C. Bettstetter, P. Grippa, H. Hellwagner, S. Sand, and S. Zhang, "Application-driven design of aerial communication networks," *IEEE Communications Magazine*, vol. 52, p. 129–137, May 2014.

[23] S. Arms, J. Galbreath, C. Townsend, D. Churchill, B. Corneau, R. Ketcham, and N. Phan, "Energy harvesting wireless sensors and networked timing synchronization for aircraft structural health monitoring," in *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, pp. 16–20, 2009.

[24] Z. Charouh and H. Chaoui, "Application of wireless networks and optical network to nextgen aircrafts," in *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)*, p. 1–2, IEEE, May 2016.

[25] J. Demo, A. Steiner, F. Friedersdorf, and M. Putic, "Development of a wireless miniaturized smart sensor network for aircraft corrosion monitoring," in *2010 IEEE Aerospace Conference*, IEEE, Mar. 2010.

[26] D.-K. Dang, A. Mifdaoui, and T. Gayraud, "Fly-by-wireless for next generation aircraft: Challenges and potential solutions," in *2012 IFIP Wireless Days*, pp. 1–8, 2012.

[27] Q. Li, M. Yang, H. Wang, Y. Jiang, and J. Zeng, "A finite queue model analysis of PMRC-based wireless sensor networks," *International Conference on Wireless Network*, pp. 30–35, 2008.

[28] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: Architectures, advances and challenges," *Ad Hoc Networks*, vol. 55, pp. 143–152, 2017. Self-organizing and Smart Protocols for Heterogeneous Ad hoc Networks.

[29] H. Sahota, R. Kumar, and A. Kamal, "Performance modeling and simulation studies of mac protocols in sensor network performance," in *2011 7th International Wireless Communications and Mobile Computing Conference*, p. 1871–1876, IEEE, jul 2011.

[30] V. Ramchand and D. Lobiyal, "An analytical model for power control t-mac protocol," *International Journal of Computer Applications*, vol. 12, p. 13–18, Dec. 2010.

[31] C. Fischione, S. Coleri Ergen, P. Park, K. H. Johansson, and A. Sangiovanni-Vincentelli, "Medium access control analytical modeling and optimization in unslotted ieee 802.15.4 wireless sensor networks," in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1–9, 2009.

[32] H. Bhatia, R. B. Lenin, A. Munjal, S. Ramaswamy, and S. Srivastava, "A queuing-theoretic framework for modeling and analysis of mobility in wsns," in *Proceedings of the 8th Workshop on Performance Metrics for Intelligent Systems*, vol. 62 of *PerMIS '08*, p. 248–253, ACM, Aug. 2008.

[33] S. N. Begum and S. Bharathidass, "Queueing theory based minimum spanning tree for energy consumption in wireless network," *International Journal of Science and Research (IJSR)*, vol. 5, no. 6, 2016.

[34] K. A. Ali and H. T. Mouftah, "Wireless personal area networks architecture and protocols for multimedia applications," *Ad Hoc Networks*, vol. 9, no. 4, pp. 675–686, 2011. Multimedia Ad Hoc and Sensor Networks.

[35] T. Qiu, F. Xia, L. Feng, G. Wu, and B. Jin, "Queueing theory-based path delay analysis of wireless sensor networks," *Advances in Electrical and Computer Engineering*, vol. 11, no. 2, pp. 3–8, 2011.

[36] R. Sámano-Robles, E. Tovar, J. Cintra, and A. Rocha, "Wireless avionics intra-communications: Current trends and design issues," in *2016 Eleventh International Conference on Digital Information Management (ICDIM)*, pp. 266–273, 2016.

[37] J. F. Schmidt, D. Neuhold, C. Bettstetter, J. Klaue, and D. Schupke, "Wireless connectivity in airplanes: Challenges and the case for uwb," *IEEE Access*, vol. 9, pp. 52913–52925, 2021.

[38] Q.-Y. Yu, H. Liu, P.-Z. Xu, J.-X. Li, L. Zhang, and H.-H. Chen, "Next generation wireless avionics intra-communications: Challenges and research topics," *IEEE Wireless Communications*, vol. 30, no. 6, pp. 87–95, 2023.

[39] Ooi and T. Chen, "Development of cdma wireless sensor network," *University Sains Malaysia*, vol. June, 2018.

[40] K. Benkic, "Proposed use of a cdma technique in wireless sensor networks," in *2007 14th International Workshop on Systems, Signals and Image Processing and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services*, pp. 343–348, 2007.

[41] E. E. Petrosky, "Receiver-assigned cdma in wireless sensor networks," Master's thesis, Virginia Polytechnic Institute and State University, 2018.

[42] I. M. Farhan, D. R. Zaghar, and H. N. Abdullah, "Performance improvement of cdma wireless sensor networks in low snr channels based on raptor codes," *Wireless Personal Communications*, vol. 130, pp. 2451–2470, Jun 2023.

[43] C. Fischione, K. H. Johansson, A. Sangiovanni-Vincentelli, and B. Zurita Ares, "Minimum energy coding in cdma wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 985–994, 2009.

[44] Y. Shudrenko, D. Plöger, K. Kuladinithi, and A. Timm-Giel, "A novel approach to enhance the end-to-end quality of service for avionic wireless sensor networks," *ACM Transactions on Internet Technology*, vol. 22, p. 1–29, Nov. 2022.

[45] A. Baltaci, S. Zoppi, W. Kellerer, and D. Schupke, "Evaluation of cellular iot for energy-constrained waic applications," in *2019 IEEE 2nd 5G World Forum (5GWF)*, p. 359–364, IEEE, Sept. 2019.

[46] C. Ghosh, "Interference mitigation in waic systems," Master's thesis, Texas A&M University, Nov 2019.

[47] GSMA, "5g and aviation altimeters co-existence with imt in 3.3-4.2 ghz and 4.8-4.99 ghz," Technical Report Page 7. 5. 5G AND AVIATION ALTIMETERS. 7., GSMA, spectrum@gsma.com; www.gsma.com, May 2023.

[48] J. Wu, Q. Li, and Y. Zhuo, "Analysis of waic qos guarantees using wireless lan technology," in *2022 21st International Symposium on Communications and Information Technologies (ISCIT)*, vol. 3, p. 76–81, IEEE, Sept. 2022.

[49] R. E. Śliwa, P. Dymora, M. Mazurek, B. Kowal, M. Jurek, D. Kordos, T. Rogalski, P. Flaszynski, P. Doerffer, K. Doerffer, S. Grigg, and R. Unnthorsson, "The latest advances in wireless communication in aviation, wind turbines and bridges," *Inventions*, vol. 7, p. 18, Jan. 2022.

[50] R. S. Robles, R. Venkatesha Prasad, A. Arts, M. Rzymowski, and L. Kulas, *Artificial Intelligence for Wireless Avionics Intra-Communications*, p. 331–352. Springer Nature Switzerland, 2024.

[51] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[52] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[53] P. Park, P. Di Marco, J. Nah, and C. Fischione, "Wireless avionics intra-communications: A survey of benefits, challenges, and solutions," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7745–7767, 2021.

[54] Q.-Y. Yu, H. Liu, P.-Z. Xu, J.-X. Li, L. Zhang, and H.-H. Chen, "Next generation wireless avionics intra-communications: Challenges and research topics," *IEEE Wireless Communications*, vol. 30, no. 6, pp. 87–95, 2023.

[55] I. Mansour, G. Chalhoub, and P. Lafourcade, "Key management in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 4, no. 3, pp. 251–273, 2015.

[56] H. Rifà-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," *Future Internet*, vol. 3, no. 1, pp. 31–48, 2011.

[57] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks," *IEEE Access*, vol. 6, pp. 11374–11387, 2018.

[58] Y. Kong, B. Lyu, F. Chen, and Z. Yang, "The security network coding system with physical layer key generation in two-way relay networks," *IEEE Access*, vol. 6, pp. 40673–40681, 2018.

[59] P. Barsocchi, S. Chessa, I. Martinovic, and G. Oligeri, "A cyber-physical approach to secret key generation in smart environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 4, pp. 1–16, Feb 2013.

[60] P. Barsocchi, G. Oligeri, and C. Soriente, "Shake: Single hash key establishment for resource constrained devices," *Ad Hoc Networks*, vol. 11, no. 1, pp. 288–297, 2013.

[61] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, (New York, NY, USA), p. 128–139, Association for Computing Machinery, 2008.

[62] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[63] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.

[64] S. T. Ben Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *2009 3rd International Conference on New Technologies, Mobility and Security*, pp. 1–5, 2009.

[65] C. Chen and M. A. Jensen, "Random number generation from multipath propagation: Mimo-based encryption key establishment," in *2009 IEEE Antennas and Propagation Society International Symposium*, pp. 1–4, 2009.

[66] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[67] X. Sun, W. Xu, M. Jiang, and C. Zhao, "Improved generation efficiency for key extracting from wireless channels," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2011.

[68] Y. E. H. Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *2011 4th IFIP International Conference on New Technologies, Mobility and Security*, pp. 1–5, 2011.

[69] G. R. Tsouri and D. Wulich, "Securing ofdm over wireless time-varying channels using subcarrier overloading with joint signal constellations," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, mar 2009.

[70] T. Kitano, A. Kitaura, H. Iwai, and H. Sasaoka, "A private key agreement scheme based on fluactions of ber in wireless communications," in *The 9th International Conference on Advanced Communication Technology*, vol. 3, pp. 1495–1499, 2007.

[71] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, 2012.

[72] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, "A wireless secret key generation method based on chinese remainder theorem in fdd systems," *Science China Information Sciences*, vol. 55, pp. 1605–1616, Jul 2012.

[73] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, pp. 1125–1133, 2011.

[74] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[75] A. Ghosal, S. Halder, and S. Chessa, "Secure key design approaches using entropy harvesting in wireless sensor network: A survey," *Journal of Network and Computer Applications*, vol. 78, pp. 216–230, 2017.

[76] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[77] W. R. Claycomb and D. Shin, "A novel node level security policy framework for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 418–428, 2011.

[78] O. Cheikhrouhou, "Secure group communication in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 115–132, 2016.

[79] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 611–622, 2013.

[80] J. C. Lee, V. C. Leung, K. H. Wong, J. Cao, and H. C. Chan, "Key management issues in wireless sensor networks: current proposals and future developments," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 76–84, 2007.

[81] Dredman, "Avsi featured in aiaa may 2017 aerospace america," Tech. Rep. ITU-R Report M.2197, AVSI-ICAO, 753 H.R. Bright Building 3141 TAMU 710 Ross Street College Station, TX 77843-3141, 979-845-5568, May 2017.

[82] P. P. Adhikari and M. Buderath, "A framework for aircraft maintenance strategy including cbm," *PHM Society European Conference*, vol. 3, jul 2016.

[83] R. Teeter, "Research and technology goals and objectives for integrated vehicle health management (ivhm)," *NASA-Contractor Report - Public*, vol. 3, October 1992.

[84] MIMOSA, "Open system architecture for condition-based maintenance," Advisory Circular FAA CFR OSA-CBM 3.3.1, MIMOSA - Open Standards for Physical Asset Management, MIMOSA, Jun 2010.

[85] B. Rapolu, "Internet of aircraft things: An industry set to be transformed," *Aviation Week Network*, vol. January, 2016.

[86] A. Mohammadnia, B. M. Ziapour, H. Ghaebi, and M. H. Khooban, "Feasibility assessment of next-generation drones powering by laser-based wireless power transfer," *Optics & Laser Technology*, vol. 143, p. 107283, Nov. 2021.

[87] M. Wu, L. Su, J. Chen, X. Duan, D. Wu, Y. Cheng, and Y. Jiang, "Development and prospect of wireless power transfer technology used to power unmanned aerial vehicle," *Electronics*, vol. 11, p. 2297, July 2022.

[88] K. Jin and W. Zhou, "Wireless laser power transmission: A review of recent progress," *IEEE Transactions on Power Electronics*, vol. 34, p. 3842–3859, Apr. 2018.

[89] S. A. H. Mohsan, H. Qian, and H. Amjad, "A comprehensive review of optical wireless power transfer technology," *Frontiers of Information Technology & Electronic Engineering*, vol. 24, p. 767–800, June 2023.

[90] D. E. Raible, "High intensity laser power beaming for wireless power transmission," *ETD Archive*, p. 167–184, Jan. 2008.

[91] H. Liu, Y. Zhang, Y. Hu, Z. Tse, and J. wu, "Laser power transmission and its application in laser-powered electrical motor drive: A review," *Power Electronics and Drives*, vol. 6, p. 167–184, Jan. 2021.

[92] J. Van Mulders, D. Delabie, C. Lecluyse, C. Buyle, G. Callebaut, L. Van der Perre, and L. De Strycker, "Wireless power transfer: Systems, circuits, standards, and use cases," *Sensors*, vol. 22, p. 5573, July 2022.

[93] SAE, "Guidelines for development of civil aircraft and systems arp4754a sec5.1, 5.2," *SAE International*, vol. Dec, 2010.

[94] IEEE-Std, "Ieee standard for low-rate wireless networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, no. 7460875, pp. 1–709, 2016.

[95] D. J. Sztrik, *Basic Queueing Theory: Foundations of System Performance Modeling*, p. 200. GlobeEdit 24 May 2016, 2016.

[96] L. Frenzel, "Fundamentals of communications access technologies: Fdma, tdma, cdma, ofdma, and sdma," Electronics Magazine M.2283-0 (12/2013), Electronics Design Magazine, © 2024 Endeavor Business Media, LLC. All rights reserved., January 2013.

[97] Digi-Newsletter, "Zigbee wifi coexistence (802.15.4 protocol and 802.11 protocol)," digi news letter, Digi International, Digi International Worldwide Headquarters, 9350 Excelsior Blvd, Suite 700, Hopkins, MN 55343, Dec 2023.

[98] U. Pešović and P. Planinšič, "Error probability model for IEEE 802.15.4 wireless communications in the presence of co-channel interference," *Phys. Commun.*, vol. 25, pp. 43–53, Dec. 2017.

[99] K. Elliott, "Development of wireless avionics intra-communications," *Avionics Today Online Magazine*, vol. June-July, 2017.

[100] T. Przybylski, N. Sugunaraj, and P. Ranganathan, "Aircraft communication systems - topologies, protocols, and vulnerabilities," whitepaper, Center for Cyber Security Research (C2SR), University of North Dakota, 2023.

[101] M. A. Simplício, P. S. Barreto, C. B. Margi, and T. C. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, vol. 54, no. 15, pp. 2591–2612, 2010.

[102] A. Baker and P. Parkinson, "Cyber security enhancements for a safety-critical arinc 653 avionics platform," in *Proceedings of the 26th Safety-Critical Systems Symposium*, February 2018.

[103] M. Ge, K.-K. R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 63, pp. 24–38, 2016.

[104] A. Ramos and R. H. Filho, "Sensor data security level estimation scheme for wireless sensor networks," *Sensors*, vol. 15, no. 1, pp. 2104–2136, 2015.

[105] L. Schrage, "A more portable fortran random number generator," *ACM Trans. Math. Softw.*, vol. 5, p. 132–138, jun 1979.

[106] S. K. Park and K. W. Miller, "Random number generators: good ones are hard to find," *Commun. ACM*, vol. 31, p. 1192–1201, oct 1988.

[107] G. Wang and W. Zhao, *The principles of integrated technology in avionics systems*. San Diego, CA: Academic Press, Jan. 2020.

[108] C. Watkins, "Integrated modular avionics: Managing the allocation of shared intersystem resources," in *2006 ieee/aiaa 25TH Digital Avionics Systems Conference*, p. 1–12, IEEE, Oct. 2006.

[109] I.-S. Suh, *Wireless charging technology*. Warrendale: SAE International, July 2015.

[110] S. K. Karan, S. Hosur, Z. Kashani, H. Leng, A. Vijay, R. Sriramdas, K. Wang, B. Poudel, A. D. Patterson, M. Kiani, and S. Priya, "Magnetic field and ultrasound induced simultaneous wireless energy harvesting," *Energy Environ. Sci.*, vol. 17, pp. 2129–2144, 2024.

[111] Reyal Yousif Osman, Aqsa Gul, A. Mohammed, and Maryiam Elnemr, "Report on the electric system design of the b787," *Report On the Electric System Design of the B787*, 2020.

[112] M. Tavana, M. Ozger, A. Baltaci, B. Schleicher, D. Schupke, and C. Cavdar, "Wireless power transfer for aircraft iot applications: System design and measurements," *IEEE Internet of Things Journal*, vol. 8, p. 11834–11846, Aug. 2021.

[113] A. Reatti, F. Corti, S. Q. Antonio, and H. P. Rimal, "Design centering of wireless power transfer systems for avionics," in *2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*, p. 1–6, IEEE, Sept. 2018.