Development and Flight Testing of a Wireless Avionics Network Based on the IEEE 802.11 Protocols

BY

Satish Kumar Chilakala

Submitted to the graduate program in Aerospace Engineering
and the Graduate Faculty of the University of Kansas
in partial fulfillment of the requirements for the degree of
Master's of Science

Chairperson ______________________________
Dr. Richard Colgren

Committee members ______________________________
Dr. David Downing

____
Dr. Mark Ewing

____
Dr. Alexander Wyglinski
Worcester Polytechnic Institute

Date Defended __01/28/2008__

The Thesis Committee for Satish Kumar Chilakala certfies

that this is the approved version of the following thesis:

Development and Flight Testing of a Wireless Avionics Network Based on the IEEE 802.11 Protocols

Chairperson ______________________________
Dr. Richard Colgren

Committee members ______________________________
Dr. David Downing

____
Dr. Mark Ewing

____
Dr. Alexander Wyglinski
Worcester Polytechnic Institute

Date Approved ____________________

Abstract

This report describes the development and flight testing of the IEEE 802.11 protocol-based Wireless Flight Management System (WFMS) using low cost Commercial-Off-The-Shelf (COTS) equipment and software.

The unlicensed spectrum allocation in the 2.4 GHz and 5 GHz bands by the FCC has encouraged the industry to develop new standards for short-range communication that are commercially viable. This has resulted in new short-range communication technologies like Bluetooth and the Wireless Local Area Network (WLAN). The new modulation techniques developed for wireless communication support wired equivalent data rates. The commercial success of these technologies and their wide market adaptation has resulted in reduced costs for the devices that support these technologies. Applications of wireless technology in aerospace engineering are vast, including development, testing, manufacturing, prognostics health management, ground support equipment and active control. The high data rates offered by technologies like WLAN (IEEE 802.11 a/b/g) are sufficient to implement critical and essential data applications of avionics systems. A wireless avionics network based on IEEE 802.11a/b/g protocols will reduce the complexity and cost of installation and maintenance of the avionics system when compared to the existing wired system.

The proposed WFMS imitates the flight management system of any commercial aircraft in terms of functionality. It utilizes a radio frequency for the transmission of the sensor data to the Cockpit Display Unit (CDU) and the Flight Management Computer (FMC). WFMS consists of a FMC, data acquisition node, sensor node and a user interface node. The FMC and the data acquisition nodes are built using PC/104 standard modules. The sensor node consists of an Attitude and Heading Reference System (AHRS) and a GPS integrated with a serial device server. The user interface node is installed with moving map software which receives data from the AHRS and GPS to display flight information including topographic maps, attitude, heading, velocity, et cetera. This thesis demonstrates the performance evaluation of the WFMS both on the ground and in flight, and its advantages over a wired system.

This thesis focuses on the evaluation of IEEE 802.11a/b/g protocols for avionics application. Efforts taken to calibrate the available bandwidth of the WLAN network at different operating conditions and varying ranges using different network analysis tools are explained briefly. Considerable research on issues like electromagnetic interference and network security critical to the development of a wireless network for avionics has also been done. This report covers different aspects of the implementation of wireless technology for aircraft systems. This work is a successful starting point for the new fly-by-wireless concept with extensions to active wireless flight control.

To my Parents and Sister

Acknowledgments

I would like to express my sincere gratitude to Dr. Richard Colgren, who has guided me and extended continuous support and encouragement throughout my thesis work. I would like to thank Dr. David Downing, Dr. Mark Ewing and Dr. Alexander Wyglinski who have agreed to be a part of my committee and have provided me with quality inputs in improving my thesis.

I would like to thank my friends Srikanth Pagadarai, Udaya Kiran Tadikonda, Shilpa Sirikonda, Padmaja Yatham, Sushma Gottimukula and Raghuram Chakravarthy for their company and immense support throughout my stay in Lawrence. I would like to thank all the SMART group members for extending their help and support. I express my thanks to Dilip Bhogadi and Suman Sadhu for collaborating with me in several technical projects. My special thanks to Amy Pabst and Andy Pichard for helping me with departmental and research work.

Last but not the least; I would like to thank my parents and sister without whom I wouldn't have been in this position. They have always been the main source of inspiration to me and will always be. Without their love and support I would not have achieved this success in my life.

Contents

List of Figures

1. Introduction

Over the past decade, the communications field has seen major breakthroughs in wireless technology. Development of new standards, such as IEEE 802.11a/b/g, and new modulation schemes have made high data rates possible. The demand for wireless devices has increased because of features such as low cost, decreased weight, and increased performance. The applications for these wireless technologies within the aviation industry are promising. The bandwidth of IEEE 802.11a/b/g wireless protocols is sufficient to support critical and essential data applications for avionics systems.

1.1. Problem Statement

This section presents different avionics data buses which are widely used in commercial aviation, to point out the need for more efficient data transfer methods for data intensive applications. Also, the IEEE 802.11 a/b/g standards and the advantages of the wireless networks are discussed.

ARINC 429 is a widely implemented data bus standard within the commercial aircraft avionics industry. It is a point-to-point link between avionics subsystems including digital electronics, air data computers, navigation systems, and engine control systems. Two buses are used for bi-directional interconnections. In a typical application, ARINC 429 buses transmit the sensor data to the flight management computer and another bus transmits the commands from the flight management computer to the sensors and systems. ARINC 429 data bus supports a data rate of 100 kbps or 12.5 kbps. With limited bandwidth and addressing capability, ARINC 429 may not be the best standard for modern avionics architectures. Military avionics use MIL-STD-1553, which supports a data rate of 1 Mbps. Unlike ARINC 429, MIL-STD-1553 is bi-directional. Another commercial avionics bus adopted as a recent industry standard is ARINC 629. It provides a multi-transmitter data bus supporting a 2 Mbps data rate. It is a relatively expensive and heavy implementation. There is always a constant need for higher data rates between the avionics subsystems.

New technologies, like ADS-B (Automatic Dependent Surveillance – Broadcast), FIS-B (Flight Information Services – Broadcast) are making aviation even safer and are improving air traffic management. This system allows pilots in the cockpit and air traffic controllers on the ground to manage aircraft traffic with greater precision. This system requires data rates in excess of 1 Mbps. It uses that bandwidth to transfer large graphical weather files, data on Temporary Flight Restrictions (TFR), and traffic in real time to the Cockpit Display of Traffic Information (CDTI). These technologies need to be integrated within current existing avionics networks which may not have been designed to support these high data rates. Implementing a wireless network based on IEEE 802.11a/b/g, rather than using cabling between the different avionics systems and sensors, greatly reduces the amount of heavy wiring and offers flexibility for future systems upgrades. More over, the supported data rates within this network are about 54 Mbps. This is 500 times faster than ARINC 429 and can accommodate data intensive applications like video, voice and data transfer over the same network. It can back up the data from flight critical systems including: engine monitoring, navigation, and airframe health monitoring systems.

1.2. Previous Work

Many demanding and efficient applications of wireless technology have attracted industry, and aviation is not an exception. The aviation industry has been relying on conventional cables with connectors, which contribute adversely to the weight of an aircraft, for connecting the different sensors and systems onboard the aircraft. Troubleshooting the wired network onboard an aircraft is a time-consuming and costly issue for the aircraft's operator. Replacing an existing avionics system is an even more difficult task. For this reason, the aviation industry is keen on the development and implementation of wireless technology as an alternative for many essential systems onboard aircraft. A wireless system would offer more flexibility, faster installation times, and simpler maintenance. There has been much research within the aviation field on the validity of wireless technology for different avionics applications. This section describes current research and developments on wireless standards within the aviation field.

The Lockheed Martin Aeronautics Company has tested the Bluetooth wireless standard on one of their F-16B test aircraft for prognostic health monitoring. For aged aircraft it is important to have structural monitoring of the airframe. It is difficult to install a wired network on an aged aircraft, and it is appropriate to use a wireless sensor network. Bluetooth is an industry standard for use as a Personal Area Network (PAN). It is also known as IEEE 802.15.1. Bluetooth uses a Frequency Hopping Spread Spectrum technique (FHSS) for data modulation and uses the 2.4 GHz ISM band. It supports a data rate of 721 Kbps in version 1.1, and up to 2.1 Mbps in version 2.0. It has a range of 10 to 100 meters based on the transmission power [2].

The NASA Dryden Flight Research Center (DFRC), along with Invocon, Inc., has developed a Wireless Flight Control System (WFCS) as a proof-of-concept. The concept was to use a radio frequency (RF) link to supplement a wired flight control connection. As a first phase of the project, a spread spectrum radio frequency data link was introduced into the flight control paths between the Flight Control Computers (FCCs) and the flight control surface actuators as shown in Figure 1.1. This concept was implemented on an F-18 Iron Bird at the DFRC test facility. The next phase would be to develop a closed-loop control system that verifies the actual control action. The goal of the WFCS is to back up a wired system and provide redundancy for enhanced safety and reliability, or to replace the wired system and decrease the size, weight, and cost of the aircraft [3][4].

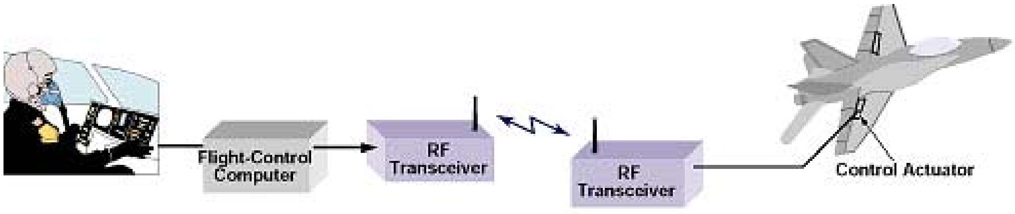


Figure 1-1: Schematic of the Wireless Flight Control System

The Ultra Efficient Engine Technology Program at the NASA Glenn Research Center is working on high temperature engine technology, which is attempting to develop high temperature wireless applications for gas turbine engines. For efficient and safe operations of the aircraft engine, continuous monitoring is required. Installing sensors for engine monitoring is a challenging task for engineers. Wireless sensors are easy to install where it is difficult to wire the moving parts of an engine [5].

Honeywell’s FliteLink wireless data management system for the Flight Data Acquisition and Management System (FDAMS) makes use of Wireless Fidelity (WiFi) and General Packet Radio Service (GPRS) networks to automatically download flight and aircraft data. This system provides fast, efficient and timely data for the airline’s flight operation, unlike the conventional way of collecting data on magnetic memory storage cards [6].

The Wireless Smoke Detection System, developed by Securaplane Technologies LLC, was the first essential wireless point-to-point intra-aircraft transmission system to get certified on a commercial airliner. The systems consists of a Central Control Unit (CCU) that receives the radio signals from smoke detection units located at different positions on the airplane. The suppression control unit (SCU) also communicates to the CCU using wireless transmission. The CCU is connected to the Control Display Unit (CDU) located in the cockpit. Figure 1.2 shows the overview of the wireless smoke detection system. The system uses spread spectrum technology for data transmission over a RF link. It reduces overall cost, installation time and weight. It was found to save 40 to 60 percent of the installation man hours when compared to the hours required for a wired system. This system is currently used by over one thousand airliners and airplanes such as the B727, B737, et cetera [7].

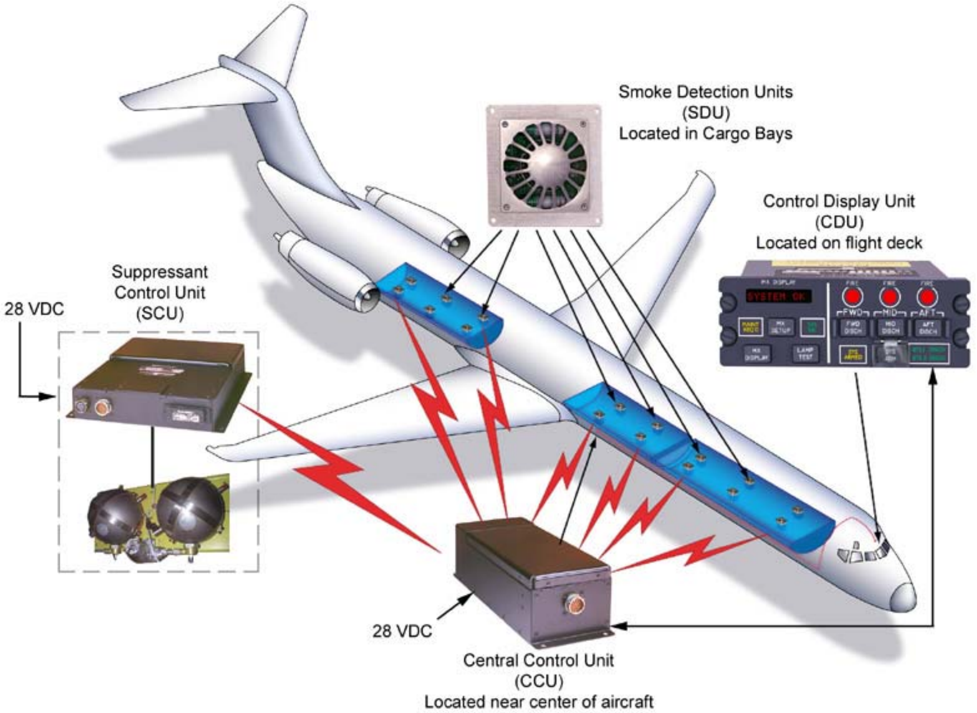


Figure 1-2: Overview of the Wireless Smoke Detection System from Securaplane Technologies

Securaplane Technologies is also developing a Wireless Emergency Lighting System (WELS) for the Boeing 787 Dreamliner. It is recognized as the world’s first wireless intra-cabin communication system to be installed and certified on a commercial airplane. The system will greatly reduce the installation weight resulting from wires.

1.3. Approach

One of the key objectives of this effort is to analyze IEEE 802.11a/b/g wireless protocols to determine if they are sufficient to support critical and essential data applications for avionics systems. If proven sufficient, wireless avionics networks based on IEEE 802.11a/b/g wireless protocols will reduce the complexity and expense of installation, maintenance, and de-installation of avionics systems as compared to existing wired systems. The current effort is to analyze these three protocols against noise level and interference to assure availability in all aircraft environments, to assess the accuracy and completeness of the data, and to demonstrate the wireless flight management system. Table 1 gives an overview of the IEEE 802.11 a/b/g protocol standards.

Standard	Modulation Scheme	Frequency Band	Data Rate	Advantages	Disadvantages
802.11a	OFDM	5 GHz UNII band	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	Less interference in the frequency band. High speed protocol	Expensive, low range
802.11b	DSSS or FHSS	2.4 GHz ISM band	1, 2, 5.5 and 11 Mbps	Longer range, Less expensive	Low speed protocol, more populated band
802.11g	OFDM or DSSS	2.4 GHz ISM band	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	Backward compatibility with 802.11b. High speed protocol	More populated band

Table 1-1: IEEE 802.11 a/b/g Protocol Standards

There are many experimental results available on the performance and behavior of IEEE 802.11a/b/g protocols, but very little is known regarding their performance within avionics or flight test applications. In this thesis, these protocols were evaluated within different operating environments. Issues including multipath, interference, and different radio sources are a concern on an aircraft. Also, the performance is to be evaluated for different modulation techniques and data rates with varying range between transmitter and receiver.

Appropriate network analysis tools are required to analyze the protocols with a greater degree of accuracy. The initial concentration of this research was to select the appropriate network analysis tools. Some open source tools were chosen which allowed us to evaluate the system's performance over a variety of transport protocols like the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

In the first stage of the research the concentration was on a two-node wireless network. Two standard laptop computers were used for performance measurements. To use any system onboard an aircraft, it has to be rugged enough to handle vibration and interference, so PC/104 and EPIC standard boards were chosen, as they are rugged and compact for use within the aircraft.

The second stage work was focused on developing and building a wireless multi-node network which emulates a viable flight management system consisting of three commercial off-the-shelf PC/104 based computers and an EPIC standard Flight Management Computer (FMC) with wireless network adapters. Sensors are connected to a wireless device server, which transfers the data to the FMC for processing. The sensors tested are the NAV420 and GPS 15. A user interface has been developed on a rugged laptop with moving map software that receives the data from the sensor node. Another node is used for data acquisition. Its prime function is to store the data from the sensors. These communications are accomplished using an IEEE 802.11 wireless link. A two node avionics network was developed between the user interface node and the sensor node for ground tests and subsequent flight testing to evaluate the performance in actual flight. Figure 1.3 shows the proposed wireless avionics system. When implemented, it offers flexibility in the placement of sensors and saves lot of weight and costs involved with wiring.

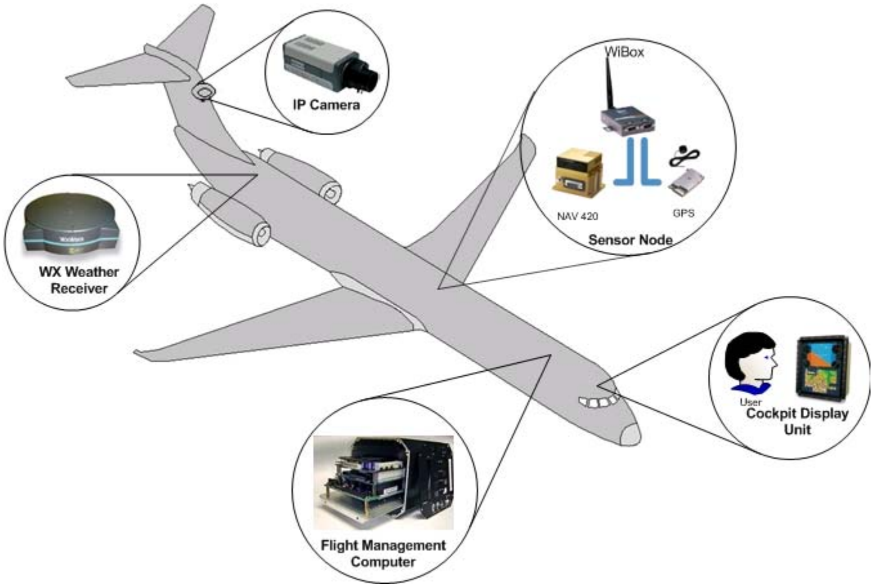


Figure 1-3: Overview of the Proposed Wireless Avionics Network

2. Background

This section gives an overview of the WLAN protocol standards. A brief description of different network analysis tools tested during this research is also given. Though there are many advantages to a wireless avionics implementation; there are also many challenges. These challenges are discussed later in this chapter.

Before going into details on wireless local area networks, an overview of the various wireless standards is required. As mentioned earlier, the unlicensed frequency allocations at 2.4 GHz and 5 GHz has encouraged the communication industry to develop new wireless standards. Among them Bluetooth, ZigBee, and WiFi are the three most popular standards. Figure 2.1 gives an overview of the various wireless standards which have developed extensive commercial application. The standards are arranged in order of increased data rate and power requirement on the X-axis, and increased operating range on the Y-axis.

It can be observed that ZigBee is at the lower end of Figure 2.1 in terms of the data rate and power requirements, making it suitable for applications like structural health monitoring where nodes can be operated on a battery power for years. There are wireless sensors like strain gauges, accelerometers, et cetera, available from various vendors, which are built using the ZigBee standard. WiMAX is at the higher end of Figure 2.1 in terms of the data rate and power requirements. WiMAX is an industry specification for the IEEE 802.16 standard. The main goal of this standard is to provide *last mile* (long range) broadband access. It uses the 2-11 GHz frequency spectrum; both licensed and unlicensed bands. It can support data rates as high as 10 Mbps at a range of 10 miles. Unlike radio frequency standards based on ZigBee, Bluetooth, WiFi, or WiMAX, there are also proprietary systems that have been developed by various vendors. Mostly, these systems are built to address specific applications or data requirements. These systems operate in the same unlicensed bands used by standards based systems (such as 915 MHz and 2.4 GHz) with a supported data rate up to 1 Mbps.

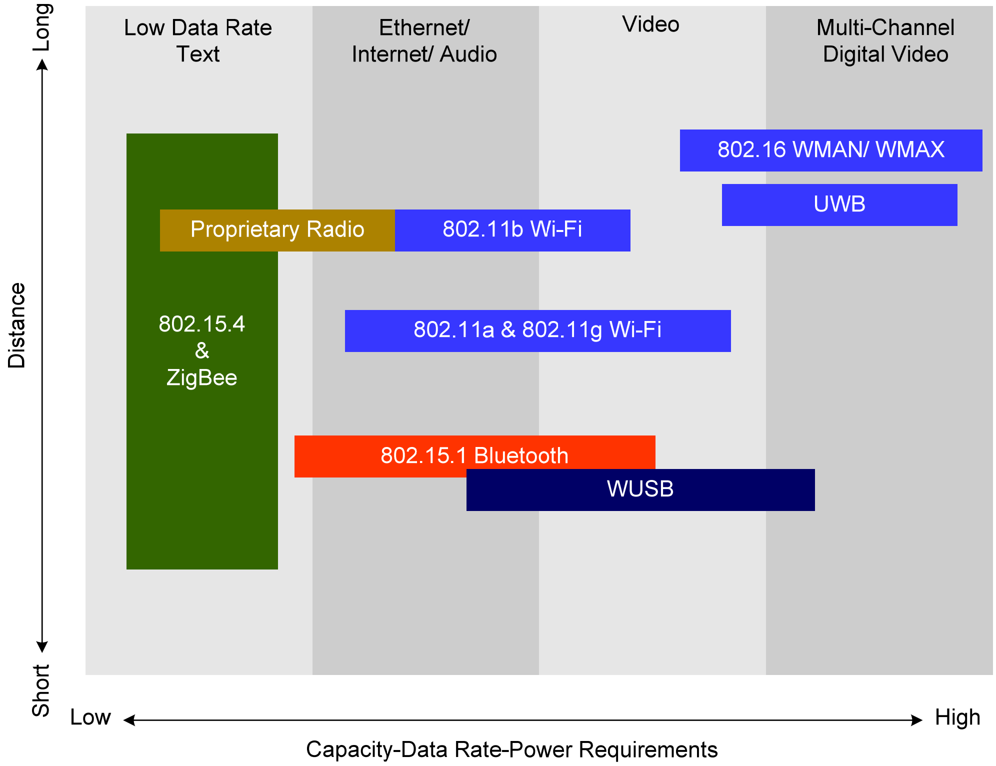


Figure 2-1: Overview of Wireless Standards [52]

WiFi, or the IEEE 802.11 standard, falls within the intermediate level of Figure 2.1. It has a high data rate (maximum of 11 Mbps for 802.11b and 54 Mbps for

802.11a/g), medium operating range, and a relatively low power requirement. This makes it suitable for avionics applications.

2.1. Wireless LAN Protocols

2.1.1. Overview

Developments in Wireless LAN (WLAN) technologies date back to the mid-1980s when the Federal Communication Commission (FCC) first made the RF spectrum available to industry [8]. The IEEE initiated the 802.11 project in 1990 and finalized the initial 802.11 standard in June 1997. The scope of this standard was to develop a Medium Access Control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area [9]. This initial standard specified three physical layer modulation schemes: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared, to support a data rates of 1 Mbps and 2 Mbps. In late 1999, the IEEE ratified the 802.11a and 802.11b high data rate wireless networking standards. The 802.11g standard was introduced later to provide the best features of both a and b standards, and to be backward compatible with IEEE 802.11b. For the past ten years, IEEE 802.11 evolved as an alternative to the wired LAN or Ethernet technology.

The IEEE 802.11 standards focus on the bottom two layers of the Open Systems Interconnection (OSI) model: the physical layer and the Data Link Layer (DLL) [10]. DLL is further divided to sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). Figure 2.2 shows the OSI model with IEEE 802.11 specified DLL and PHY layers.

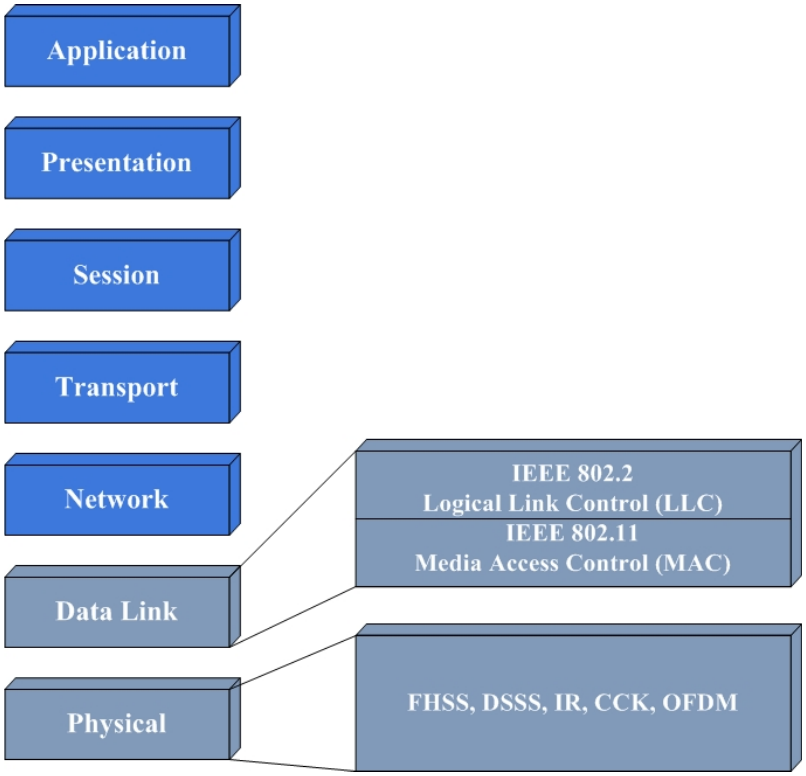


Figure 2-2: IEEE 802.11 Specification of the OSI Model

The goal of the MAC layer is to provide reliable data delivery for the upper layers over the wireless PHY media. It is also responsible for maintaining order in the use of shared medium. IEEE 802.11 uses a distributed MAC protocol based on Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) as a channel access mechanism. CSMA/CA is similar to the collision detection access method specified in 802.3 Ethernet LANs [11]. In this access technique, when a node wants to transmit, it first listens to the medium or channel to ensure no other node is transmitting. If the radio channel is clear, it starts transmitting. Otherwise, it will wait for a random amount of time (backoff interval) before listening again to verify a clear channel for transmission. This technique works efficiently in LANs where the network traffic is low.

As mentioned earlier, the original IEEE 802.11 standard specified three modulation schemes in the PHY. Two of them are based on spread spectrum technology. In the 802.11a and 802.11g standards, a new modulation scheme called Orthogonal Frequency Division Multiplexing (OFDM) was introduced. It improves the spectrum efficiency and supports higher data rates (54 Mbps, in practice this rate is not achieved). The OFDM scheme is resilient to RF interference and has lower multipath distortion than the DSSS and FHSS modulation schemes. The specifications for the IEEE 802.11a/b/g protocols are given in the following sections.

2.1.2. IEEE 802.11a

IEEE 802.11a is a very high-speed, high-bandwidth standard. It is a variant of the IEEE 802.11 standard. Devices using the IEEE 802.11a standard operate in the 5 GHz Unlicensed National Information Infrastructure Band (UNII). In the USA there are three permitted frequency ranges within the 5 GHz frequency band: 5.15 GHz-5.25 GHz, 5.25 GHz-5.35 GHz, and 5.725 GHz-5.825 GHz. Within this band there are twelve 20 MHz channels, with different transmitting power limits for each band. IEEE 802.11a uses OFDM, a new encoding scheme that offers benefits over the use of the spread spectrum technique in channel availability and data rate. The IEEE 802.11a standard contains seven data rates (6, 9, 12, 18, 24, 36, 48 Mbits/s); however, maximum rates of 54 Mbits/s are common. Each data rate uses a particular modulation technique to encode the data. Higher data rates are achieved by employing advanced modulation techniques. Since the 2.4 GHz band is heavily used, the 5 GHz band gives IEEE 802.11a the advantage of less interference but has the disadvantage of reduced operational range. Figure 2.3 shows eight 20 MHz channels within the two lowest frequency bands.

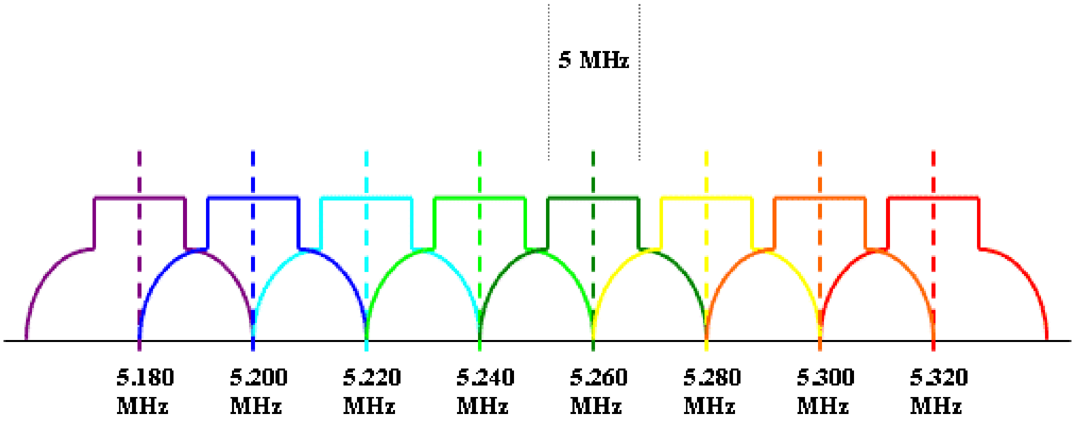


Figure 2-3: IEEE 802.11a Channels in the 5 GHz Frequency Band

2.1.3. IEEE 802.11b

The IEEE 802.11b specification was the first widely accepted wireless networking standard. The IEEE 802.11b standard provides location-independent access to an outside network through wireless data devices, including intercommunication on a local scale. Devices using the IEEE 802.11b standard operate within the 2.4 GHz band, which is divided into fourteen 22 MHz channels, eleven of which legally operate in the US. Adjacent channels partially overlap, except for three of the 14 (1, 6, 11), which are completely non-overlapping. The IEEE 802.11b standard utilizes a Direct Sequence Spread Spectrum (DSSS) modulation mode and an advanced coding technique (Complementary Code Keying) to achieve higher data rates of 5.5 Mbit/s and 11 Mbit/s. The data rates degrade to either 2 Mbits/sec or 1 Mbits/sec if substantial interference is present. The coding techniques employ different modulation schemes at different data rates. A range of 100 meters is typical, but ranges are dependent upon environmental obstacles and power. Figure 2.4 shows eleven channels of 22 MHz bandwidth in the 2.4 GHz frequency band. Channels 1, 6 and 11 are non-overlapping.

2.1.4. IEEE 802.11g

The IEEE 802.11g standard has been developed to extend the speed and range beyond the IEEE 802.11b standard. This standard operates entirely within the 2.4 GHz frequency bands, but uses a minimum of two mandatory modes with two optional modes. It employs different modulation techniques for different data rates. The modulation scheme employed in IEEE 802.11g is OFDM for data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts (like the IEEE 802.11b standard) to CCK for 5.5 and 11 Mbit/s, and to DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. Data rates of 6 to 54 Mbits/s are possible. IEEE 802.11g is interoperable with IEEE 802.11b, as they operate within the same frequency band. Despite its major acceptance, IEEE 802.11g suffers from the same interference problem as IEEE 802.11b within the already crowded 2.4 GHz range. Devices operating within this frequency range include microwave ovens, Bluetooth devices, and cordless telephones.

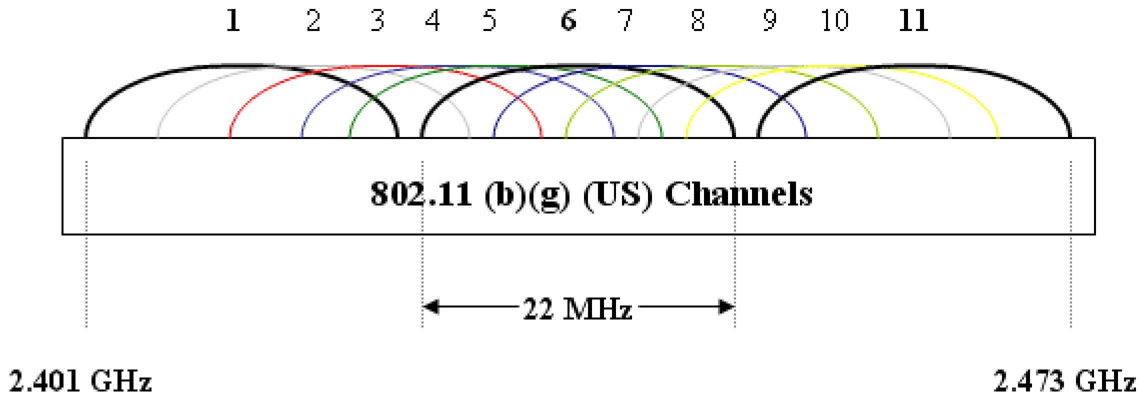


Figure 2-4: IEEE 802.11b/g Channels in the 2.4 GHz Frequency Band

2.2. Wireless LAN Topologies

The IEEE 802.11 standard defines three basic topologies to be supported by the MAC layer implementation:

- Independent Basic Service Set (IBSS) or Ad-Hoc Mode
- Basic Service Set (BSS) or Infrastructure Mode
- Extended Service Set (ESS)

2.2.1. Independent Basic Service Set

In a wireless network, Ad-Hoc mode, referred to as IBSS topology, is a method for wireless devices to communicate directly with each other. Ad-Hoc mode allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion without involving a central relay system or access points. Every client may not be able to communicate with every other client due to the range limitation. If a client in an Ad-Hoc network wishes to communicate outside of the peer-to-peer cell, a member must operate as a gateway and perform routing. Figure 2.5 shows the Ad-Hoc network in which all the stations communicate with each other directly.

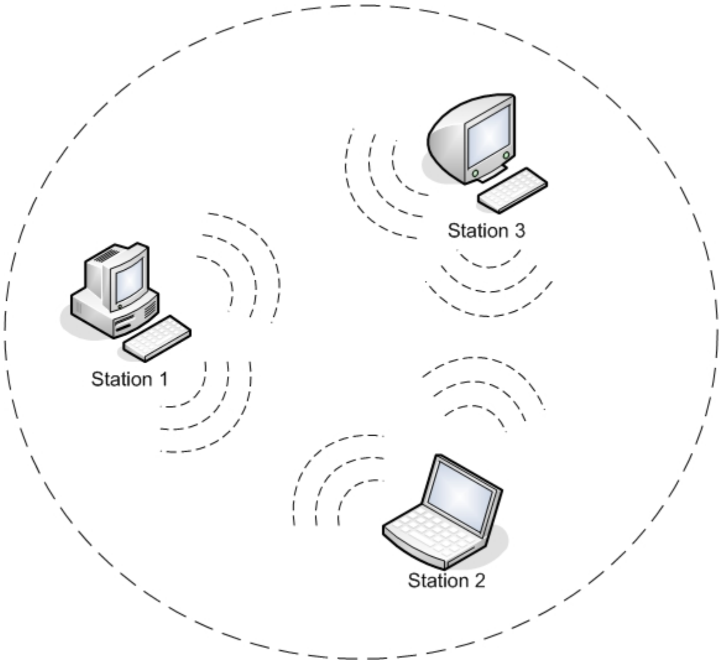


Figure 2-5: Schematic of the Ad-Hoc Network Topology

Ad-Hoc mode does not require an access point and it is easier to set up, especially in a small or temporary network. All wireless adapters in the Ad-Hoc network must use the same SSID and the same channel number to be able to communicate with each other. However, there are some disadvantages when employing Ad-Hoc mode. Interference increases as the number of devices grows, because all the devices use the same frequency channel, affecting their performance. Ad-Hoc networks cannot bridge to wired LANs or to the internet without installing a special-purpose gateway. Multiple computers will connect to pass the data between systems that are out of range, causing significant network delays. It is also difficult to secure an Ad-Hoc network because of its flexible design.

2.2.2. Basic Service Set

The Basic Service Set is an alternative topology to the IBSS. It is also known as the Infrastructure mode. It overcomes the obstacles experienced using the Ad-Hoc mode. This mode requires the use of a wireless Access Point (AP). All frames are relayed between the wireless clients by the access point, and no direct communication is supported. Before being able to communicate data, wireless clients and AP’s must authenticate and establish a relationship. Only then can two wireless clients exchange data. AP’s provide a simple means of hardware bridging between the wireless and wired components of the network. An infrastructure wireless network provides a more reliable network connection for wireless clients. Figure 2.6 shows the WLAN in infrastructure mode, with the associated wireless access point. The AP is connected to the backbone network.

Even though use of a AP would be expected to add to the cost of implementing a wireless networking solution it can be highly beneficial, especially when there is a plan to add new users. Complex IEEE 802.11 networks may be built using the infrastructure mode, with the advantage of scalability, centralized security management, and improved range.

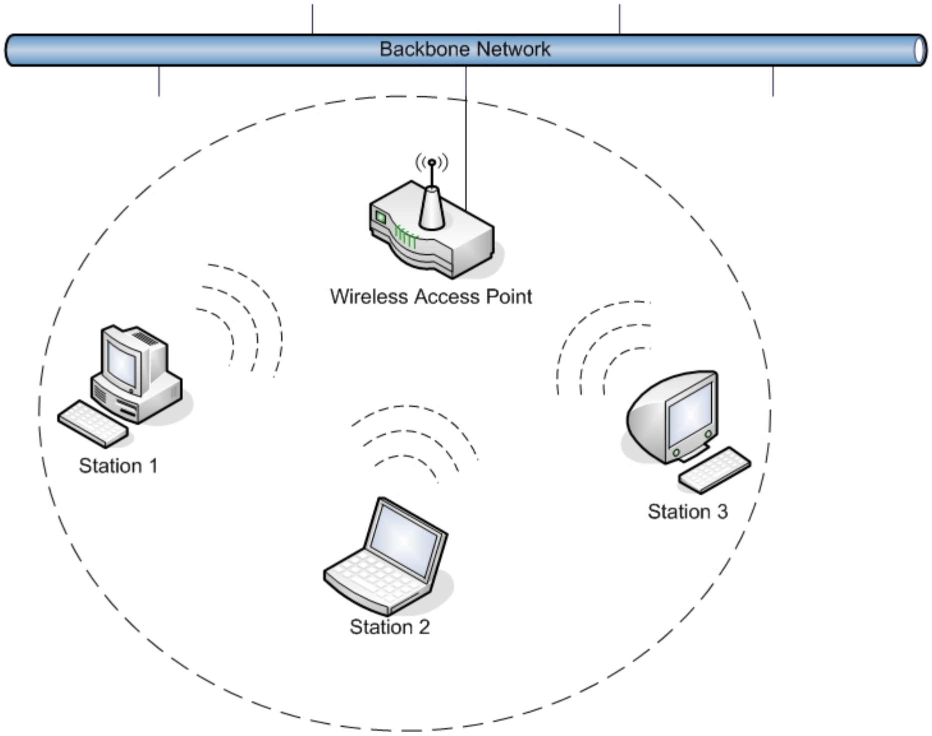


Figure 2-6: Schematic of the Infrastructure Network Topology

It is possible to combine multiple wireless access points into a single sub-network, referred to as an ESS topology. It is thus possible to expand the wireless network with multiple AP's utilizing the same channel, or to utilize different channels to boost aggregate throughput.

2.3. Wireless Network Security

The difference between the wired and wireless network is the medium through which the data is transferred. In wired networks, unauthorized access can be prevented by physical security [9]. Wireless networks use radio frequency for communication, so they are more susceptible to security attacks. This is because of their broadcast nature and the lack of physical barriers. These issues assume special prominence when WLANs are applied to avionics networks. Typically, attacks on network security are divided into *passive* and *active* attacks [8]. A passive attack is one in which an unauthorized person gains access to the network but does not modify the content. Attacks like eavesdropping and traffic analysis fall under this category. Attacks such as masquerading, replay, man-in-the-middle attack, and denial-of-service, in which the attacker actually modifies the content, are known as active attacks. These kinds of attacks lead to loss of confidentiality, loss of integrity, and loss of network availability. Basic methods to improve security include: avoiding the broadcast beaconing of the SSID, applying MAC address filtration to restrict the network access to only limited clients based on their physical address, et cetera. It is necessary to address different kinds of security features and the encryption standards that would make the network robust to possible attacks. This section gives an overview of the various security standards developed for IEEE 802.11 networks to overcome security vulnerabilities.

2.3.1. Wired Equivalent Privacy (WEP) Algorithm

The IEEE 802.11 specification identified several services to provide a secure operating environment. Wired Equivalent Privacy (WEP) was an encryption algorithm designed to provide link-level authentication between the clients and access points during wireless transmission [8]. IEEE 802.11 does not provide either end-to-end or user-to-user authentication [9]. The original IEEE 802.11 standard was defined with three kinds of security features to secure the wireless data transmission given in the following sections.

2.3.1.1. Authentication

The IEEE 802.11 specification allows two ways to validate client attempts to gain access (access control) to the network. These are known as open system authentication and shared key authentication. In an open system, any station (client) can get authenticated by an access point without the identity of the station being verified. Shared key authentication requires implementation of the WEP algorithm. Since there is no cryptographic technique in open system authentication, it is more vulnerable to security attacks than shared key authentication.

2.3.1.2. Privacy

The IEEE 802.11 standard supports privacy through the encryption techniques supported by WEP. WEP uses the RC4 symmetric key, stream cipher algorithm. Since it is a stream cipher, a seed value is required to start its key stream generator. This seed is called the Initialization Vector (IV). As per the specification in the

802.11 standard, WEP supports only 40-bit encryption keys for the shared key. The IV and the shared WEP key are used to encrypt the data. The sender XORs (Exclusive OR) the stream cipher with the plaintext, which is the actual data attached to the Integrity Check Value (ICV), to produce ciphertext. The ciphertext is then forwarded to the receiver along with the IV in the plaintext. The receiver uses this IV and the WEP key to decipher the packet. The security of the encryption standard can be increased by increasing the key size. Research has shown that key sizes of greater than 80-bits make brute-force code breaking an impossible task, with the possible number of keys being greater than 10^{26} [8].

2.3.1.3. Integrity

One of the goals of WEP is to provide a means to check the data integrity for messages transmitted in a wireless LAN. This service was designed to reject any messages that have been modified by an unauthorized person. WEP uses an encrypted Cyclic Redundancy Check (CRC) value to provide data integrity. For each packet before ciphering, a CRC is computed and attached to the payload. This packet is then ciphered and transmitted. The receiver deciphers the packet and the CRC is recomputed on the received message. The CRC computed from the data at the receiver is compared with the one that was received in the packet. If the CRCs do not match, an integrity violation is indicated and the packet is discarded.

2.3.2. Vulnerabilities in WEP

It is found that WEP is not as secure as was once believed. WEP is used only at the link layer and physical layers of the OSI model, and does not offer end-to-end security [12, 13]. Some of the vulnerabilities in implementing WEP algorithm are as follows [14]:

Poor Key Management – WEP uses a static key in the sense that the WEP key is typed into a wireless device to be associated with a wireless network. The same key is used by all the users in the network to enable WEP. There is no mechanism to renew the stored WEP key. Since all the wireless devices use the same WEP key for encryption, a large amount of traffic may be available to an eavesdropper for cracking the key.

WEP Key Recovery – WEP uses the static key and a different IV to encrypt data. The IV, a 24-bit field with a limited range (0 to 16,777,215) to choose from, is sent in the plaintext form along with the cipher text. Eventually, the same IVs may be used over and over again in a relatively short time in a busy network [8]. Reuse of the same IV produces identical key streams for encryption. Once enough data is collected, the WEP key can be cracked by an attacker.

Unauthorized Decryption and the Violation of Data Integrity – WEP doesn't provide a cryptographic integrity protection. IEEE 802.11 uses a non-cryptographic CRC to check the integrity of packets. Once the WEP key is revealed, an attacker will have access to the cipher text. By using the WEP key, the data can be read or modified.

Access Point Authentication – The authentication method provided by WEP is only one-way. The wireless clients are authenticated in the network. But there is no way that the access point is authenticated. The wireless clients must trust that it is communicating to a real access point.

To address security issues in WEP, many third-party solutions, such as: Virtual Private Networks (VPN), enhanced and dynamic WEP key, and the IEEE 802.1X standard for authentication, were introduced. IEEE 802.1X is a port-based network access control standard, adopted by the 802.11 working group for authentication, authorization, and key management [14, 15]. It uses the Extensible Authentication Protocol (EAP) for user-level authentication. For better key management, IEEE 802.1X employs dynamic, per-station or per-session key management and provisions for rekeying.

2.3.3. Wi-Fi Protected Access (WPA)

Based on the demands for more secure solutions in implementing WLAN, the Wi-Fi alliance, in conjunction with IEEE, developed Wi-Fi Protected Access (WPA) before the final security standard IEEE 802.11i standard was ratified. WPA is a standards-based interoperable security specification [14] which is a subset of the security features specified in the IEEE 802.11i standard (also known as WPA2) [16]. WPA provides a strong encryption algorithm along with per user authentication, which was missing in WEP. A simple software or firmware upgrade would suffice for the existing hardware to support WPA. It is designed to be forward and backward compatible with IEEE 802.11i and WEP standards, respectively. The key features of the WPA standard are as follows:

2.3.3.1. Authentication

WPA adopts the 802.1X specification with EAP to address issues with mutual authentication. A combination of an open system and 802.1X are used by WPA. With EAP, 802.1X uses a Remote Authentication Dial-In User Service (RADIUS) authentication server in an enterprise environment. EAP provides the users' credentials, unique usernames and passwords, and extended authentication methods [16]. Because of the dynamic key management and rekeying supported by EAP, the wireless access point can change the encryption key periodically, preventing key determination attacks. For an environment with no provision for RADIUS, WPA employs a pre-shared key mechanism for user authentication.

2.3.3.2. Encryption

To address the vulnerabilities in data encryption using WEP, the Temporal Key Integrity Protocol (TKIP) scheme was derived from 802.11i [14]. The key size is increased from 40-bits in WEP to 128-bits. Unlike the WEP key, where an 24-bit initialization vector and 40-bit WEP key are used to generate a key stream, TKIP uses an 48-bit initialization vector and the MAC address of a wireless client with the 128-bit temporal key that is shared among the clients and the access points [17]. It also provides dynamic generation of the keys, with which the temporal keys are changed every 10,000 packets and key distribution is achieved by the use of an authentication server [17]. The usage of key hierarchy and management methods exchanges WEP’s single static key for some 500 trillion possible keys, preventing key prediction [16]. In spite of the strong security features offered by TKIP over WEP, the use of the RC4 algorithm for encryption makes it a temporary solution [14].

2.3.3.3. Integrity

WPA provides data integrity using a Message Integrity Code (MIC), also referred to as a “Michael” algorithm [18]. The IEEE 802.11 standard specified the use of a 4-byte Integrity Check Value (ICV) that is appended to the 802.11 packets. The receiver calculates the ICV of the received frames to determine whether the received ICV is the same as the calculated value. Although the ICV is encrypted by WEP, it is possible to modify the bits in the encrypted frames without this action being detected by the receiver. Using the Michael algorithm, WPA calculates an 8-byte MIC and places it between the data and the 4-byte ICV of the 802.11 frame and encrypts it before transmission. The Michael algorithm also provides a new frame counter to prevent replay attacks [15].

With a firmware upgrade, WPA offers a good solution to enhance security within the WLAN. Though there have been no successful attacks, WPA has potential encryption weaknesses with TKIP. A better encryption technique is specified in WPA2, which is the second generation of WPA security.

2.3.4. Wi-Fi Protected Access 2

Wi-Fi Protected Access 2 (WPA2) was introduced to formally replace WEP and the other security features of the original 802.11 standard [20]. WPA2 is based on the IEEE 802.11i amendments ratified in June 2004 [19]. As with WPA, WPA2 supports 802.1X with EAP or Pre-Shared Key (PSK) technology mutual authentication, and Michael message integrity code for strong data integrity. WPA2 employs the Advance Encryption Standard (AES) algorithm for data encryption.

2.3.4.1. Advanced Encryption Standard

IEEE 802.11i includes the new advanced encryption technique using the counter-mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) Protocol (CCMP) called the Advanced Encryption Standard (AES) [19]. AES counter mode is a block cipher that uses an 128-bit encryption key and encrypts 128-bit blocks of data at a time, using the Rijndael algorithm. AES meets the Federal Information Processing Standard (FIPS) 140-2 requirement [20], and has been approved by the United States government for encrypting sensitive and unclassified information. AES supports three key sizes: 128-bit, 192-bit and 256-bit with approximately 1.1 x 10^{77} possible keys for a selected 256-bit key [21]. A hardware upgrade is required to existing wireless devices to implement AES.

Wi-Fi Protected Access 2 provides a robust solution to all the vulnerabilities known in WEP. It offers a much stronger encryption technique and enhances data protection and integrity in the WLAN.

2.4. Network Analysis Tools

The primary goal of this work was to measure different performance metrics for a wireless network based on the IEEE 802.11a/b/g protocols under different operational conditions. The key performance metrics are throughput, round trip time, data loss, etc. Many open source network analysis or monitoring tools are available for measuring these metrics [27]. In this section some of the widely used network analysis tools that have been examined are discussed.

2.4.1. Ethereal

Ethereal is an open source software released under the GNU General Public License and runs on most Unix and Unix-compatible systems, including: Linux, Solaris and Windows. It is a protocol analyzer or packet sniffer used for network troubleshooting, analysis, and software and protocol development. It allows the user to see all the traffic being passed over a network. The functionality *Ethereal* provides is very similar to *tcpdump*, but it has a GUI front-end, and many more information sorting and filtering options. Here are some of its features [22]:

- Data can be captured "off the wire" from a live network connection, or read from a captured file.
- Live data can be read from Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM, and loopback interfaces (at least on some platforms; not all of those types are supported on all platforms).
- Captured network data can be browsed via a GUI.

- Captured files can be programmatically edited or converted via command-line switches to the *editcap* program.
- 759 protocols can be analyzed.

2.4.2. Iperf

Iperf is open source software developed by the National Laboratory for Applied Network Research (NLANR). It is a tool to measure IP bandwidth using the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). It enables the tuning of the system parameters and the UDP characteristics. It supports IPv6 and multicast. *Iperf* floods a connection with small packets and measures the time to send a quantity of data, predicting system data transfer speeds. *Iperf* reports bandwidth, delay jitter, and datagram loss. Some of the key features of *Iperf* are as follows [23]:

- Measure TCP bandwidth
- Report MSS/MTU size and observed read sizes
- Support for TCP window size via socket buffers
- Client and server can have multiple simultaneous connections
- UDP Client can create UDP streams of a specified bandwidth
- Measure packet loss
- Measure delay jitter
- Multicast capable

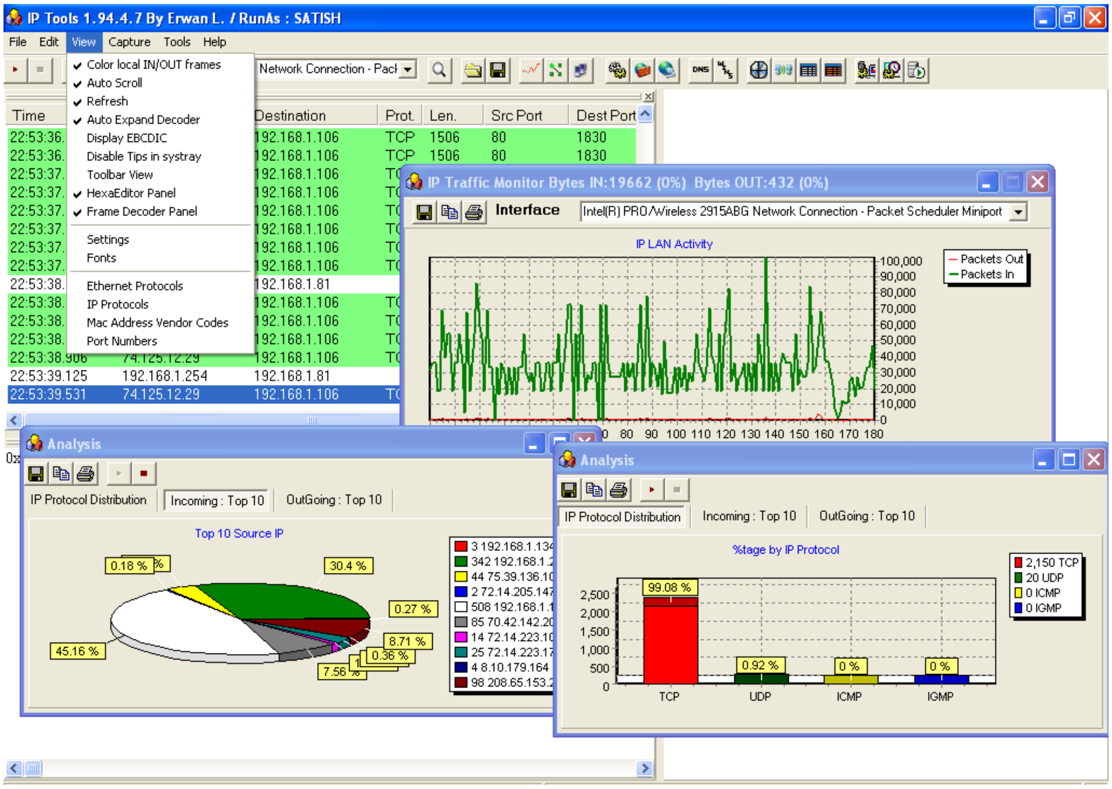
2.4.3. tcptrace

The *tcptrace* software is a TCP Connection Analysis Tool originally written by Dr. Shawn Ostermann at Ohio University. It can take the files produced by several popular packet-capture programs as input, including: *tcpdump*, *snoop*, *etherpeek*, and *WinDump* [24]. The *tcptrace* software can produce several different types of output containing information on each connection such as: elapsed time, bytes and segments sent, received retransmissions, round trip times, window advertisements, throughput, and more. It can also produce a number of graphs for further analysis.

The *tcptrace* software can generate six different types of graphs illustrating various parameters of a TCP connection. These graphs can be viewed with the *xplot* program or with the Java version of the same program called *jPlot* [26]. It can produce detailed statistics on the TCP connections from *dumpfiles* under the long output option. *TCPdump/tcptrace/xplot* is a widely used software combination.

2.4.4. IP Sniffer

IP sniffer is a suite of IP Tools built around a packet sniffer, developed by Erwan’s Lab. It uses *WinPCap* or the *NDIS* protocol to facilitate packet capture. *IP Sniffer* can be used to analyze and troubleshoot networks. It has features such as: bandwidth monitoring, traceroute, protocol analysis, port scanning, et cetera [25]. Figure 2.7 shows the graphical interface. *IP Sniffer* was used in the flight test of the wireless avionics network to monitor the network performance and is mentioned in later sections.



```
Time           Destination    Prot. Len.  Src Port  Dest Port
22:53:36.      192.168.1.106  TCP   1506  80        1830
22:53:36.      192.168.1.106  TCP   1506  80        1830
22:53:37.      192.168.1.106  TC
22:53:37.      192.168.1.106  TC
22:53:37.      192.168.1.106  TC
22:53:37.      192.168.1.106  TC
22:53:37.      192.168.1.106  TC
22:53:37.      192.168.1.106  TC
22:53:38.      192.168.1.81
22:53:38.      192.168.1.106  TC
22:53:38.      192.168.1.106  TC
22:53:38.      192.168.1.106  TC
22:53:38.906   74.125.12.29   192.168.1.106  TC
22:53:39.125   192.168.1.254  192.168.1.81
22:53:39.531   74.125.12.29   192.168.1.106  TC
```

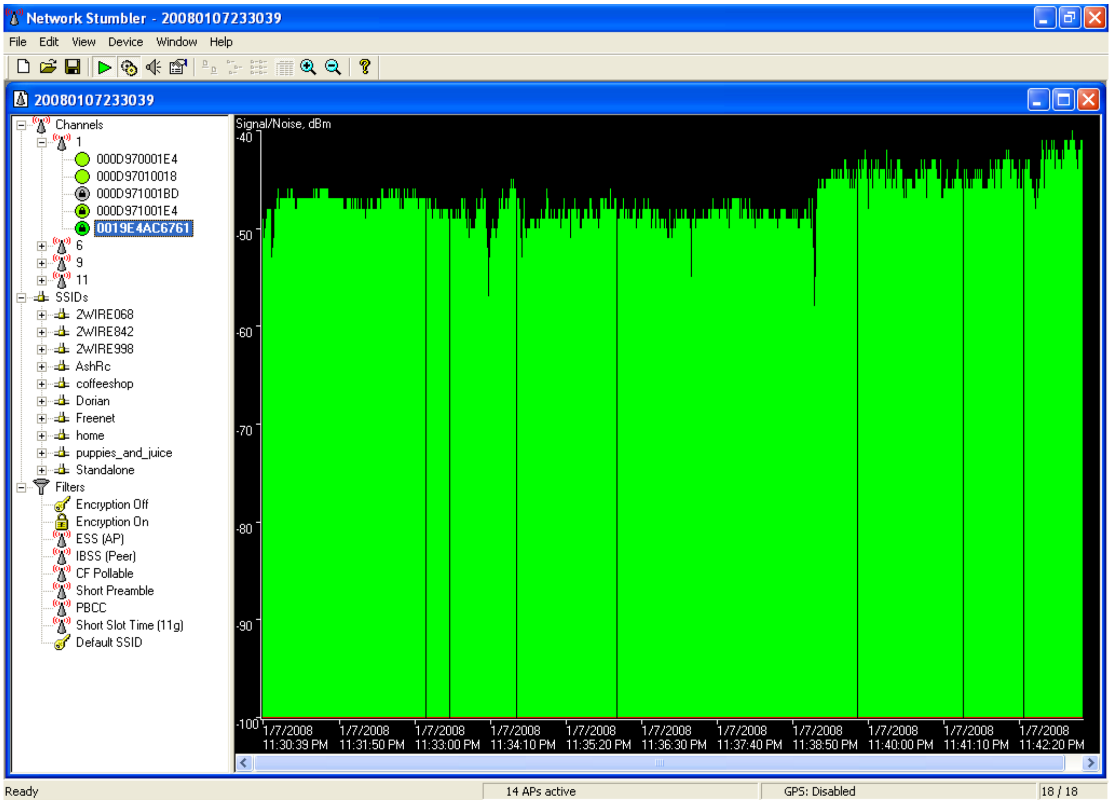
🟥	3 192.168.1.134
🟩	342 192.168.1.2
🟨	44 75.39.136.10
🟦	2 72.14.205.147
□	508 192.168.1.1
▨	85 70.42.142.20
🟪	14 72.14.223.10
▨	25 72.14.223.17
🟦	4 8.10.179.164
🟫	98 208.65.153.2

🟥	2,150 TCP
🟩	20 UDP
🟨	0 ICMP
🟦	0 IGMP

Figure 2-7: Graphical Interface of IP Sniffer Software

2.4.5. NetStumbler

NetStumbler is a tool for Windows that allows us to detect WLANs using IEEE 802.11a/b/g standards [28]. *NetStumbler* can be used to find locations with poor coverage in the WLAN, to detect "rouge" access points in the workplace, and to detect other networks that may be causing interference. It sends a probe request to all the access points it found approximately once every second, and reports the response. Using *NetStumbler*, the radio environment in the vicinity of the WLAN can be analyzed. Figure 2.8 shows a screenshot of the *NetStumbler*'s user interface. The green bars indicate the signal strength in dBm. Higher bars indicate stronger signal strength. *NetStumbler* was used to determine the signal strength of the wireless avionics network under various operating conditions.



Ready | 14 APs active | GPS: Disabled | 18 / 18

Figure 2-8: Graph-View of NetStumbler Software

2.5. Electromagnetic Interference (EMI)

One of the main concerns in implementing wireless technology onboard an aircraft is interference. There is possible EMI with the onboard radio and navigation equipment with these WLAN devices. Therefore, we need to analyze the electromagnetic environment around these devices within different aircraft radio frequency bands. It also helps us understand any kind of noise induced in the data transmission that could affect the performance of the WLAN devices.

The bandwidth of IEEE 802.11 protocols is sufficient to support essential and critical applications for avionics systems. However, there is not much data available to prove their robustness and their ability to provide the accuracy and availability necessary to support aircraft safety requirements. Also, the safety issues involved in using new wireless COTS equipment within the aircraft environment needs to be investigated. Potential EMI due to spurious radio emissions from these wireless systems on the aircraft's radio and navigation equipment needs to be verified. Prior to that, some background on different aircraft radio and navigation systems is required.

The antenna frequency bands used by the aircraft's avionics systems span the electromagnetic spectrum from a few kilohertz to several thousand megahertz. At the very low end of the spectrum is the old Omega navigation system, which operates in the frequency range of 10-14 kHz. At the very high end is the weather radar system, which operates at 5,440 and 9,350 MHz [29]. Some of the aircraft's systems and their frequency range of operation are shown in Table 2.1.

Frequency Range	**System**
190-1750 kHz	Automatic Direction Finder (ADF)
2-30 MHz	High Frequency (HF) Radio
75 MHz	Marker Beacon
108-112 MHz	Localizer (LOC)
108-118 MHz	VHF Omnidirectional Range (VOR)
118-137 MHz	Very High Frequency (VHF) Radio
329-335 MHz	Glide Slope
962-1213 MHz	Distance Measuring Equipment
1030, 1090 MHz	Air Traffic Control (ATC)
1030, 1090 MHz	Traffic Alert and Collision Avoidance (TCAS)
1530-1660 MHz	Satellite Communication (SATCOM)
1575.42 MHz	Global Position Satellite (GPS)
4235-4365 MHz	Radio Altimeter
5031-5091 MHz	Microwave Landing System (MLS)
5440, 9350 MHz	Weather Radar

Table 2-1: Different Avionics Communication and Navigation Bands [27]

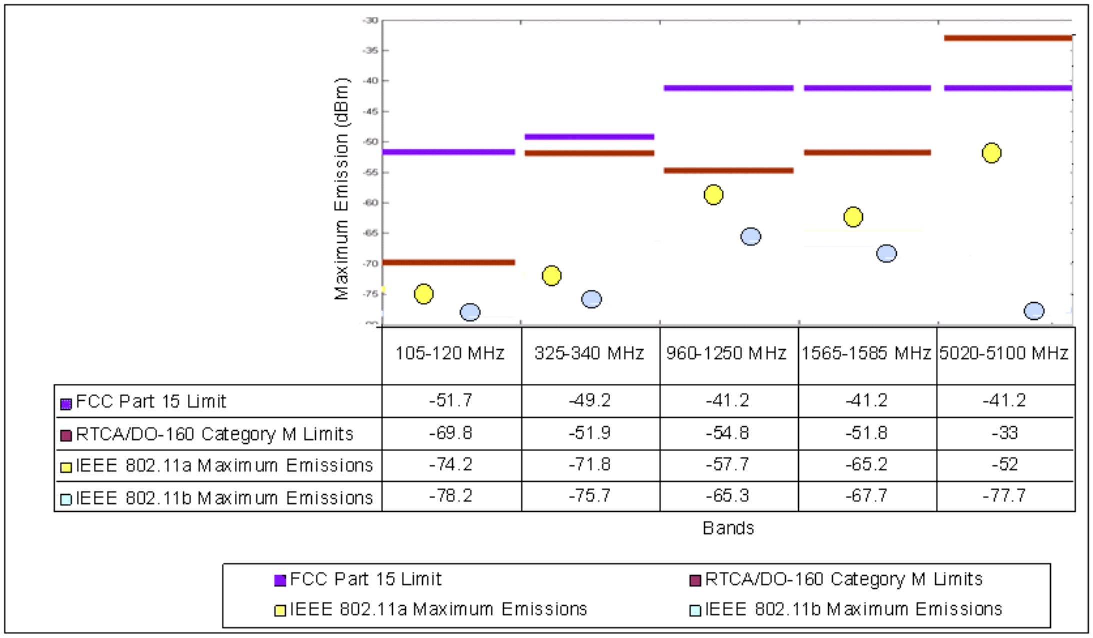
Spurious emissions are emissions outside of the actual radio frequency of the device. There have been many concerns about passengers carrying Portable Electronic Devices (PED), such as laptops, Personal Digital Assistants (PDA) and mobile phones, onboard an aircraft that could interfere with the aircraft’s radio and navigation equipment. NASA has done some experimental studies under the NASA Aviation Safety Program with the support of the FAA Aircraft Certification Office. Aircraft interference path loss measurements were conducted for various aircraft radio receivers on four B747-400 and six B737-200 aircraft [29, 30]. A radiated emission measurement process was developed, and spurious radiated emissions from various devices were characterized using reverberation chambers. Spurious radiated emissions within aircraft radio frequency bands from several WLAN devices are compared with the baseline emissions from standard laptops and PDAs. From the receiver interference threshold data provided by RTCA/DO-199 and the IPL, an interference risk assessment from these WLAN devices was made.

The radiated emissions from the WLAN devices were measured within a reverberation chamber at the NASA LaRC. The WLAN devices tested include seven IEEE 802.11b and five IEEE 802.11a devices. The preliminary testing was done with different WLAN operating modes, channels, and data rates. Five frequency bands were selected for the initial testing. Band 1 to Band 5 covered many aircraft radio bands of interest, including: Instrument Landing System (ILS), LOC, VOR, GS, TCAS, Air Traffic Control Radar Beacon System (ATCRBS), Distance Measuring Equipment (DME), GPS, and the Microwave Landing Systems (MLS). In later tests VHF Communications were also added. Table 2.2 explains the frequency bands covered, along with the avionics system using that band.

Measurement Band Designation	Measurement Freq. Range (MHz)	Aircraft Systems Covered	Spectrum (MHz)
Band 1	105-120	LOC	108.1-111.95
		VOR	108-117.95
Band 1a	116-140	VHF-Com	118-138
Band 2	325-340	GS	328.6-335.4
Band 3	960-1585	TCAS	1090
		ATCRBS	1030
		DME	962-1213
		GPS L2	1227.60
		GPS L5	1176.45
Band 4	1565-1585	GPS L1	1575.42 ± 2
Band 5	5020-5100	MLS	5031-5090.7

Table 2-2: Different Frequency Bands Tested [29, 30]

The data presented in the PED and WLAN device envelope comparison indicated that radiated emissions from the WLAN devices were less than PED emissions. There was one exception in Band 5 (5020 MHz-5100 MHz), where the emissions from WLAN devices were more than that of PED. This could be because the transmission frequency of IEEE 802.11a devices is close to the Band 5 frequency. MLS is the only system operating within this band. It was concluded that the risk to the MLS system was low, as there are no installed MLS systems within the US. In Figure 2.9 the maximum emission values from IEEE 802.11a and 802.11b devices are compared to the FCC Part 15 Limits and the RTCA/DO-160 Category M Limits.



	105-120 MHz	325-340 MHz	960-1250 MHz	1565-1585 MHz	5020-5100 MHz
🟪 FCC Part 15 Limit	-51.7	-49.2	-41.2	-41.2	-41.2
🟥 RTCA/DO-160 Category M Limits	-69.8	-51.9	-54.8	-51.8	-33
🟨 IEEE 802.11a Maximum Emissions	-74.2	-71.8	-57.7	-65.2	-52
□ IEEE 802.11b Maximum Emissions	-78.2	-75.7	-65.3	-67.7	-77.7

Figure 2-9: EMI Test Results Compared with RTCA Standards

3. Overview of the Wireless Flight Management System

In this section, the development of a network architecture for the wireless flight management system, and the different elements of the system, are described. Details of the different hardware components constituting the different nodes within the network are given.

3.1. Flight Management Computer

An EPIC standard-based wireless node was developed to act as a Flight Management Computer (FMC). This system was tested within a two-node network, measuring the performance of the WLAN protocols. This wireless node was developed using a 1.4 GHz Pentium-M processor SBC from Ampro Computers Inc. stacked with an EnGenius NL-5354MP mini-PCI card on a Mesa 4I67 dual type III mini PCI adapter and a Tri-M HESC-104 50W power supply. The system was enclosed within a PC/104 enclosure purchased from Diamond Systems. The system was developed to use an 8 GB compact flash as a storage device. This system acts as a flight management computer within our wireless avionics network. Figure 3.1 shows the PC/104 form factor on an EPIC standard SBC within the enclosure.

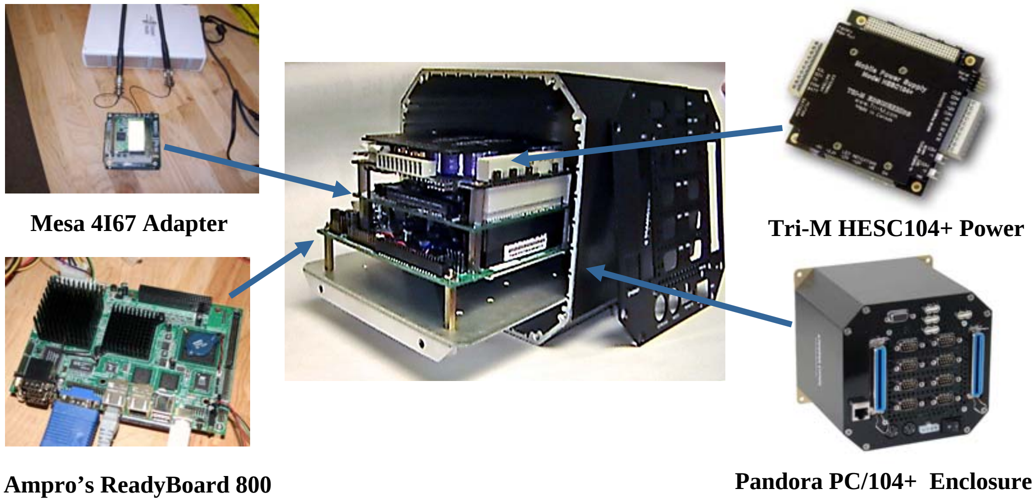


Figure 3-1: EPIC based Flight Management Computer

3.2. Data Acquisition and Sensor Node

Within the wireless avionics network, the remaining nodes require less computing power than the FMC. They are developed on a PC/104-plus form factor. The different modules incorporated within the system are described within the following sections.

3.2.1. Single Board Computer (SBC)

The highly integrated CoreModule™ 600 PC/104-*Plus* compatible SBC features an ultra low power 400MHz ULV Celeron, advanced networking, high performance graphics and other state of the art embedded PC features [44]. The CoreModule™ 600 is ideal for compact, size-conscious, high volume, rugged embedded designs that require higher performance at a reasonable cost. Figure 3.2 shows the CoreModule™ 600.

Figure 3-2: CoreModule™ 600

3.2.2. Wireless Adapter

The 4I67 is an adapter that allows use of 2 MINI-PCI type III cards, for example wireless network cards, on a PC/104-PLUS host CPU [45]. The 4I67 shown in Figure 3.3 uses a PCI bridge so that the 4I67 only occupies a single PC/104 slot. An EMP-8602 Wireless Mini PCI card from EnGenius Technologies has been used in our system. It supports the IEEE 802.11a/b/g protocols.

Figure 3-3: 4I67 Mini PCI Adapter

3.2.3. Analog to Digital Converter

The Diamond-MM-16-AT from Diamond Systems has been employed as an Analog to Digital Converter (ADC) [48]. Figure 3.4 shows the Diamond-MM-16-AT ADC. The 16-bit analog input channels on the ADC feature programmable gains of 1, 2, 4, and 8, as well as a programmable unipolar/bipolar range, for a total of 9 different input ranges with a maximum sampling rate of 100 KHz. The board also has four 12-bit D/A channels with multiple unipolar and bipolar output ranges. It has an onboard timer to control A/D sampling or rate generator functions, 8 digital inputs, and 8 digital outputs.

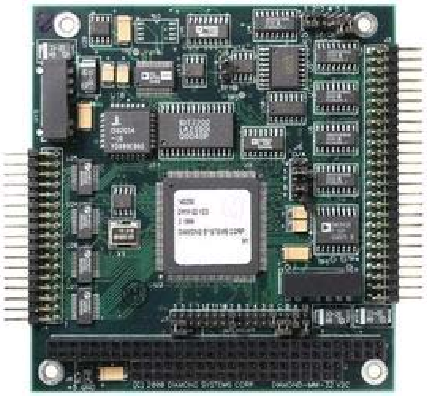


Figure 3-4: Diamond-MM-16-AT ADC

3.2.4. Power Supply

The HE104-512-16 from Tri-M Systems and Engineering Inc. is a rugged, extended-temperature DC/DC power supply designed specifically for mobile PC/104 computing applications [46]. It consists of a PC/104 form factor module with complete DC/DC voltage regulator circuitry, heat sink, input and output connectors, power-good indicator, and both 8-bit and 16-bit PC/104 bus headers. Figure 3.5 shows the PC/104 power supply from Tri-M Systems.

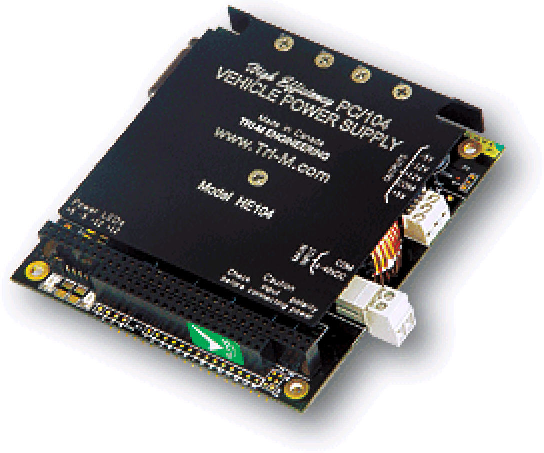


Figure 3-5: HE104-512-16 PC/104 Power Supply

3.2.5. PC/104 Enclosure

The Can-Tainer shown in Figure 3.6 is a rugged PC/104 enclosure system constructed of 0.125" aluminum and is designed for hostile and mobile environments [46]. It features a dual system of shock and vibration isolation. The PC/104 modules are mounted axially in the enclosure with four internal rubber corner rails to absorb high-frequency vibrations, while the entire enclosure is mounted on the host platform with a thick rubber pad which absorbs low-frequency G-forces.

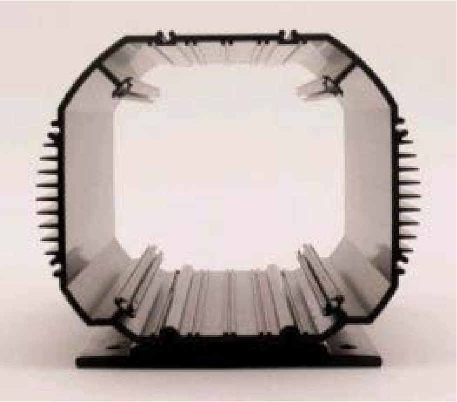


Figure 3-6: Can-Trainer PC/104 Enclosure

3.3. Sensor Node

3.3.1. Attitude and Heading Reference System (AHRS)

Recent MEMS technology developments have seen a breakthrough in avionics sensors. Low cost solid state instruments based on MEMS technology have many applications within the general aviation industry. For our initial testing, we have used the NAV420 MEMS based Attitude Heading Reference System (AHRS) and have integrated it within the wireless avionics network [42].

AHRSs are typically integrated into Electronic Flight Information Systems (EFIS), which form the central part of so-called "glass cockpit" installations. The NAV420 from Crossbow Technologies, shown in Figure 3.7, is a low-cost, solid-state GPS Inertial Measurement Unit (IMU) and navigation system that incorporates measurements from its GPS, Micro Electro-Mechanical System (MEMS) gyros and accelerometers, and fluxgate magnetometers to provide a navigation solution at a 100 Hz output rate. Together, the GPS, inertial sensors, and magnetometers provide data on the aircraft’s six degrees of freedom: horizontal, vertical, depth, pitch, yaw, and roll. The NAV420 is less than one-tenth the size and one-tenth the cost of most tactical or navigation-grade inertial systems. Instead of bulky mechanical dampers, the NAV420 relies on high-order hardware and digital filters to dampen the high-frequency sensor response. These systems can provide general aviation aircraft with a compact, light-weight, reduced INS solution that can handle aircraft vibrations.

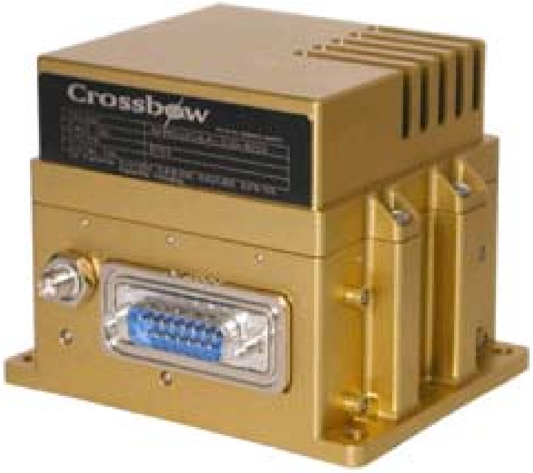


Figure 3-7: NAV420CA-200

The NAV420 provides stand-alone solutions for AHRS and integrated GPS/IMU applications. The NAV420 has two bi-directional asynchronous serial ports to support user interaction. The user port facilitates reading navigation and AHRS output packets and other data requested by the user through the NAV420's input communication protocol. The user port also supports user configuration and magnetic calibration of the NAV420. The GPS port allows National Marine Electronics Association (NMEA) standard GPS messages to be read directly. It also supports the sending of custom GPS configuration commands. The NAV420 can be set to output one of the three types of data: scaled sensor packet, angle packet, and NAV packet. These packets contain 34, 34, and 36 bytes of data, respectively.

3.3.2. Serial Device Server

A serial device server is one that is able to read data from a serial device via a RS-232 cable and is able to transmit the data to the network. The initial network architecture using a PC/104 single board computer as the device server was replaced with a new architecture using a WiBox® as the serial device server [49]. The proposed architecture presents several advantages, as the WiBox dual-port device server enables connection of equipment to IEEE 802.11b/g wireless networks or Ethernet via serial ports. It also greatly simplifies the connectivity of the devices within applications where mobility is required or cabling is impractical. Serial RS-232/422/485 flexibility, advanced security, robust data handling capabilities and high serial speeds, coupled with ease of installation and maintenance, make the WiBox a smart alternative to the PC/104 based serial device manager. The infrastructure mode architecture consists of the sensor node (NAV420 with GPS) being connected to an access point of the network wirelessly through the WiBox. Figure 3.8 shows the functional diagram of the sensor node with the NAV420 and the GPS connected to the two serial ports of the WiBox device server. With the use of the WiBox, there is no further need for additional programming to connect other serial devices to the network. The WiBox is also capable of encrypting the data read from the serial ports by 128 or 256 bit Rijndael AES Encryption before the data being communicated is sent wirelessly to the access point. The wireless network can be protected by WiFi Protected Access (WAP, WAP2). The configuration of the WiBox with the AHRS and the user interface node is described in Chapter 5.

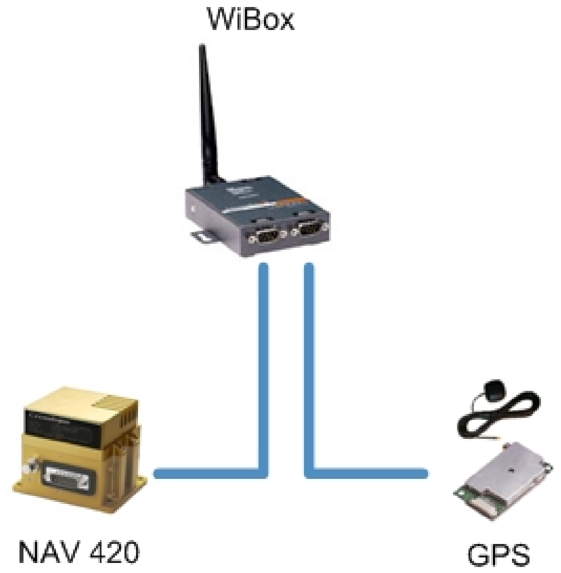


Figure 3-8: Functional Diagram of the Wireless AHRS Unit

3.3.3. Wireless AHRS Unit

The NAV420 was integrated with WiBox to act as the wireless sensor node, and was made a standalone unit by including an independent 12V DC power source. The unit was installed in the Can-Tainer, which is a rugged PC/104 enclosure system constructed of 0.125" aluminum and is designed for hostile and mobile environments. Figure 3.9 shows the components of the wireless AHRS.

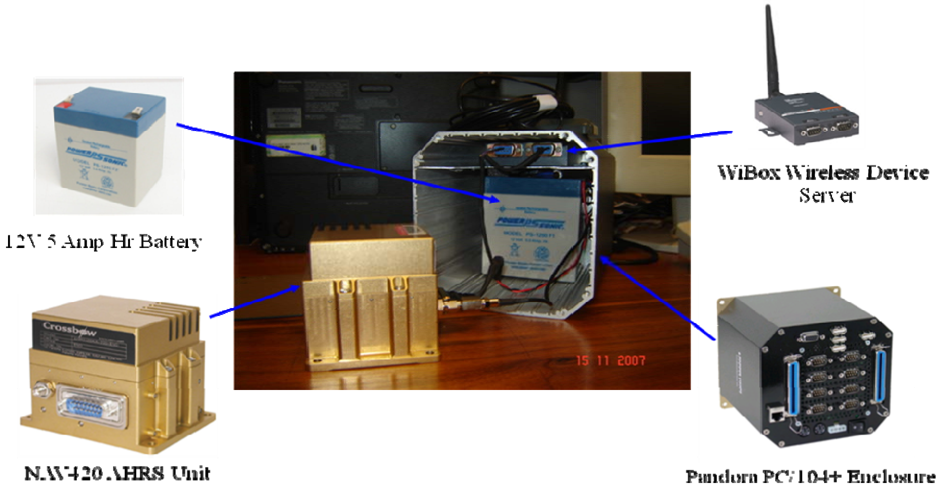


Figure 3-9: Self-Contained Wireless AHRS Unit

3.4. User Interface Node

The user interface node is located within the cockpit for the pilot's reference and it duplicates the functions of a cockpit display unit. Different commercially available moving map software systems were evaluated to emulate a cockpit display unit on a rugged laptop for use during the flight testing. The MountainScope software from PCAvionics was selected for this user interface node. It obtains position and velocity information in real-time from the GPS and displays information including a moving map which notes high resolution terrain, class B/C/D/E airports, color shaded terrain warnings, et cetera. It also reads data from the NAV420 to show the pitch and roll attitudes. Figure 3.10 shows a screen shot of the MountainScope software when tested in our laboratory with the GPS 15L. Some additional features of this software include the ability to conduct flight planning, simulate localizers, display graphical weather information, temporary flight restrictions, etc.

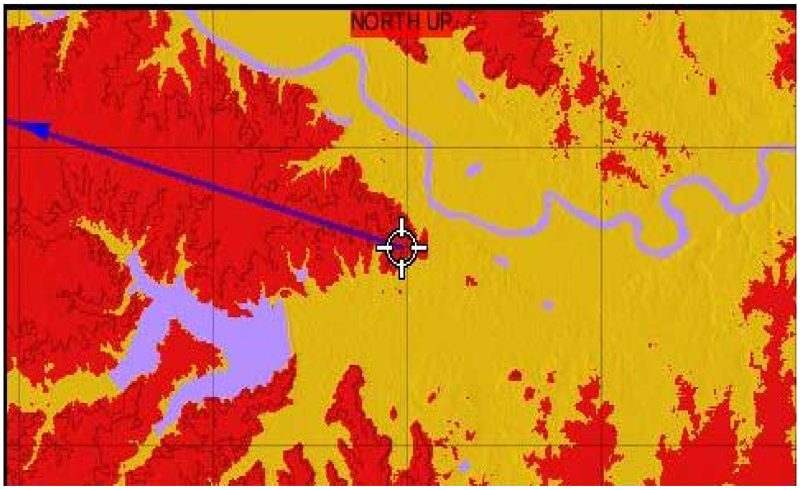
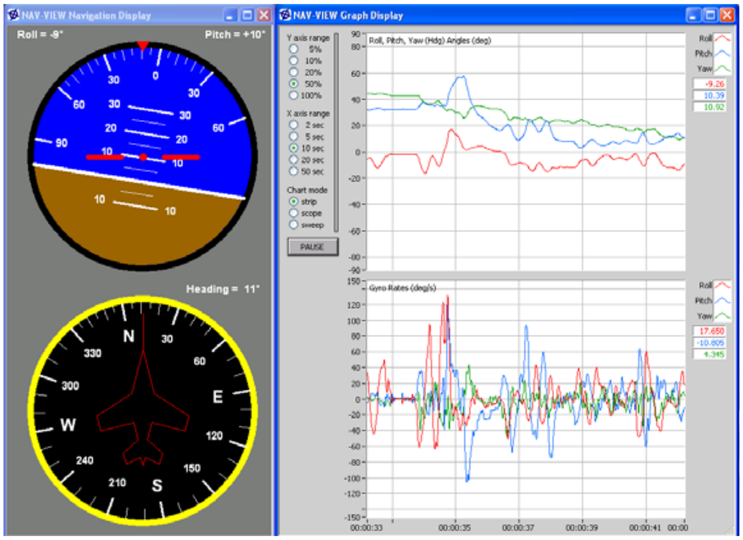


Figure 3-10: Screenshot of the MountainScope Display Showing the Color Shaded Terrain

The NAV-VIEW software from Crossbow has also been used on this project to display the pitch, roll and heading angles and rates from the NAV420 on the user interface node.



NAV-VIEW Navigation Display

Roll = -9°
Pitch = +10°
Heading = 11°

NAV-VIEW Graph Display

Y axis range
○ 5%
○ 10%
○ 20%
● 50%
○ 100%

X axis range
○ 2 sec
○ 5 sec
● 10 sec
○ 20 sec
○ 50 sec

Chart mode
● strip
○ scope
○ sweep

PAUSE

Roll -9.26
Pitch 10.39
Yaw 10.92

Roll 17.650
Pitch -10.805
Yaw 4.345

Figure 3-11: Graphical View of Navigation Data from NAV-VIEW

When connected to the NAV420, NAV-VIEW also emulates the actual attitude and course indicators. Figure 3.11 shows this display as tested in our laboratory. Using such a system, the pilot is provided with situational awareness of the aircraft's flight attitude and heading.

3.5. Network Architecture

To build a successful wireless network it is important to have a good network architecture which clearly defines the various elements of the network. In a wired flight management system, sensors such as an Attitude and Heading Reference System (AHRS) and an Air Data Computer (ADC) use a combination of RS-232, ARINC 429 or RS-485 interfaces to connect with the flight management computer or the avionics processing unit. In our wireless network, we achieve a similar architecture, where the AHRS unit and GPS talk to the user display unit and the flight management computer using WiFi.

As described in the previous chapter, WiFi supports two main network topologies; namely, infrastructure and ad-hoc modes. In infrastructure mode, all the nodes are associated with an access point, and this access point can route the data between the nodes or onto a backbone wired (Ethernet) network. In Ad-Hoc mode, the communication is peer to peer, in the sense that nodes can talk to the each other directly without the aid of any access point. There can also be hybrid topologies depending on the application.

By examining the current application, an infrastructure mode has been adopted, and the network architecture has been developed. Figure 3.12 shows the schematic view of the wireless avionics network in the infrastructure mode. Sensor nodes consist of a NAV420 and a GPS connected to a WiBox device server. All network elements are associated with the wireless access point. The Wibox sends the raw data from the sensors to the network through the access point.

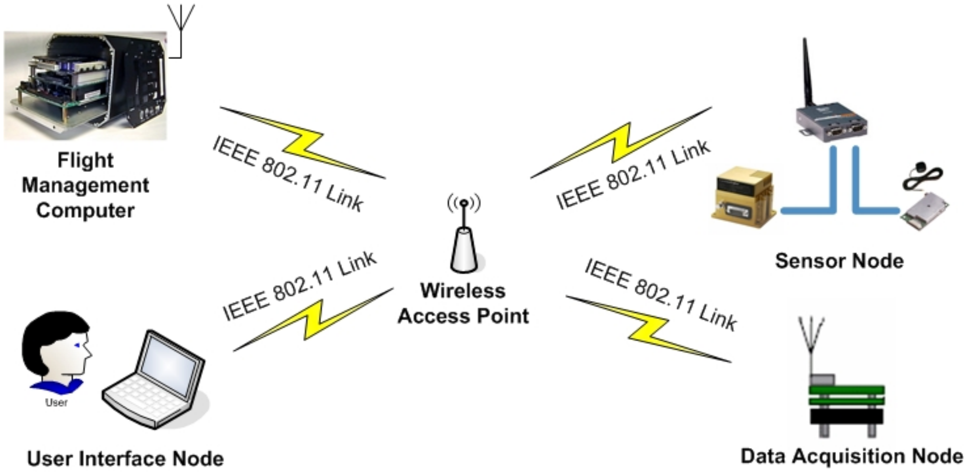


Figure 3-12: Wireless Flight Management System Architecture

4. Performance Evaluation of Wireless LAN Protocols

Evaluation of different performance metrics for the IEEE 802.11 protocols with respect to range and environment is very important to find the bandwidth supported by these protocols at varying ranges. A two node wireless network has been developed to measure throughput and round trip time using the wireless link between them. This section describes the test procedure for the evaluation of these protocols.

4.1. Test Setup

The primary goal of these experiments was to establish a wireless connection between two nodes using IEEE 802.11a/b/g wireless protocol standards, and to measure network performance at varying ranges. The Ad-Hoc network was developed between the user interface node and the Flight Management Computer (FMC). Figure 4.1 shows the developed network setup. The experiments were conducted at four different ranges (25 ft, 75 ft, 150 ft and 275 ft). Channels 1 (2.412 GHz) and 11 (2.462 GHz) were evaluated at these different range settings. *Iperf, Tcptrace,* and *Tcpdump* network analysis tools were used for these tests. The output files from *Tcptrace* were plotted using *jPlot.*

The experiment was repeated in both indoor and outdoor environments. The test procedure followed was as described:

- Iperf was installed on both nodes.

- Two nodes were separated by a range of 25 ft, 75 ft, 150 ft and 275 ft.
- Two nodes were set in Ad-Hoc mode.
- SSID was set to “abc” for both the nodes.
- Operational channels tested were 1 and 11 (2.412 GHz and 2.462 GHz) for IEEE 802.11g and channel 64 (5.32 GHz) for IEEE 802.11a.
- FMC was placed under client mode and the laptop in server mode.
- Run time was set to 20 seconds.
- Ten test runs were conducted at each range.

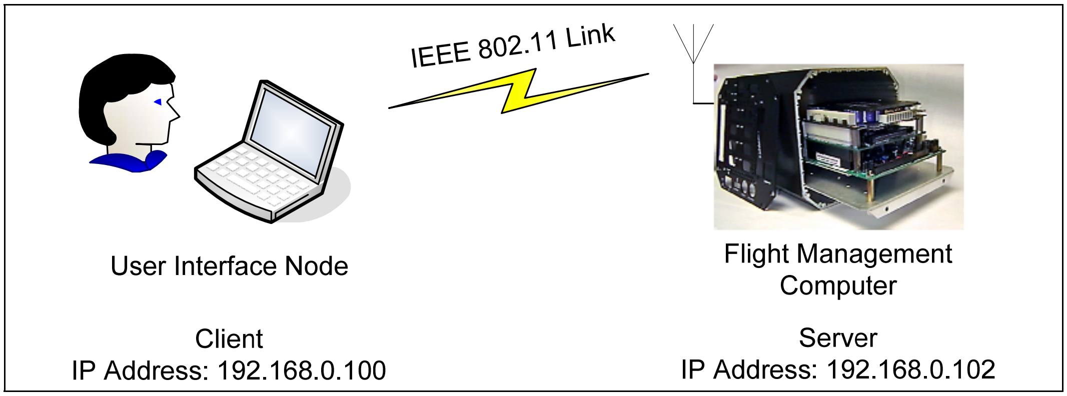

IEEE 802.11 Link
User Interface Node
Client
IP Address: 192.168.0.100
Flight Management Computer
Server
IP Address: 192.168.0.102

Figure 4-1: Two Node Network Test Setup

Different test runs were conducted in both of these environments and the results were tabulated. To get a better measure of performance, an average of ten values were taken at each distance. Figures 4.2 and 4.3 show the bandwidth variation across trials using channels 1 and 11 in the 2.4 GHz band. Different trial numbers are shown on the X-axis, and bandwidth in Mbits/sec is shown on the Y-axis. It can be estimated from the figures that the IEEE 802.11g protocol supports a consistently high data rate (14 Mbps) over a range of at least 150 ft. Both channels 1 and 11 show similar performance at varying ranges. Figures 4.4 and 4.5 indicate bandwidth variations at different range test trials.

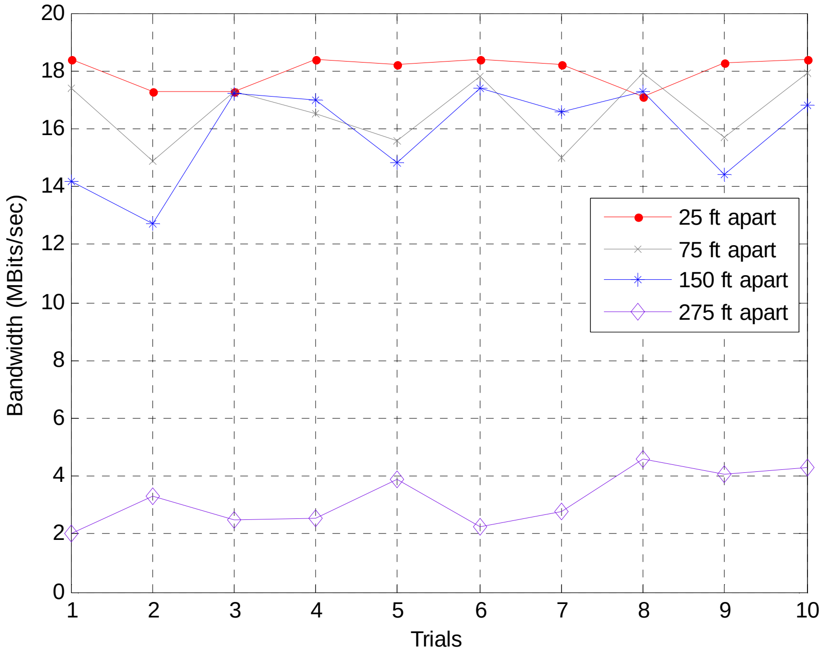


Figure 4-2: Bandwidth Measurement for IEEE 802.11g Channel 1 (2.412 GHz)

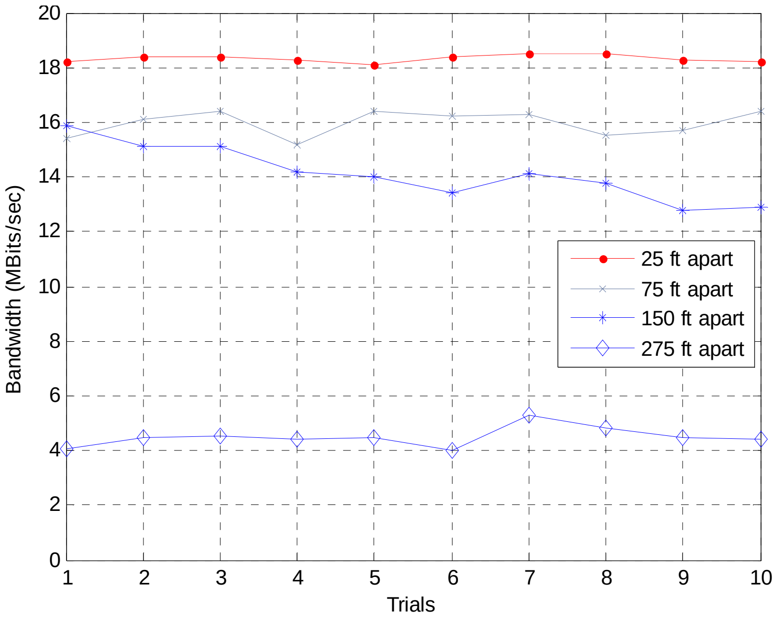


Figure 4-3: Bandwidth Measurement for IEEE 802.11g Channel 11 (2.462 GHz)

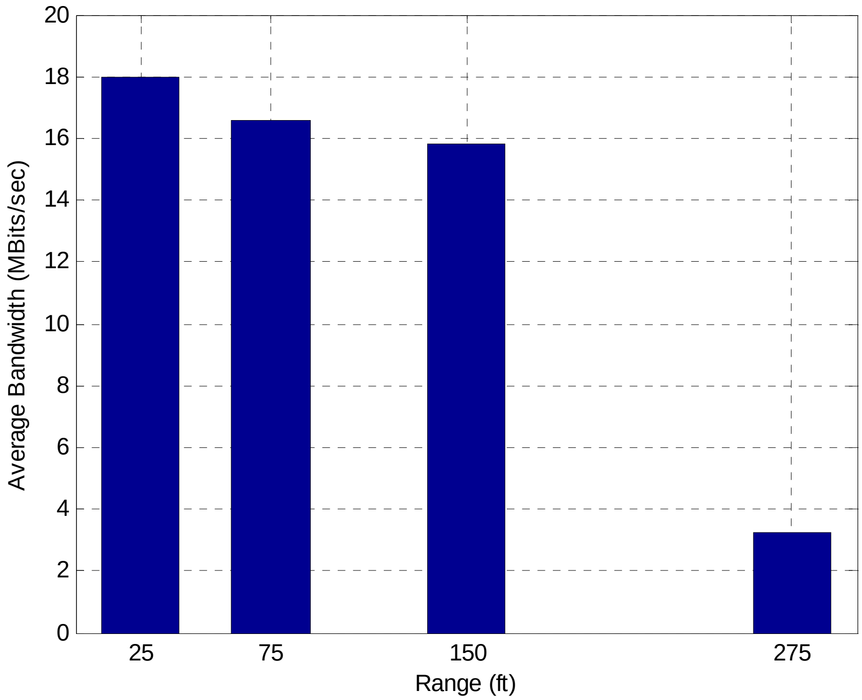


Figure 4-4: Bandwidth Variation for IEEE 802.11g Channel 1 (2.412 GHz) with Range

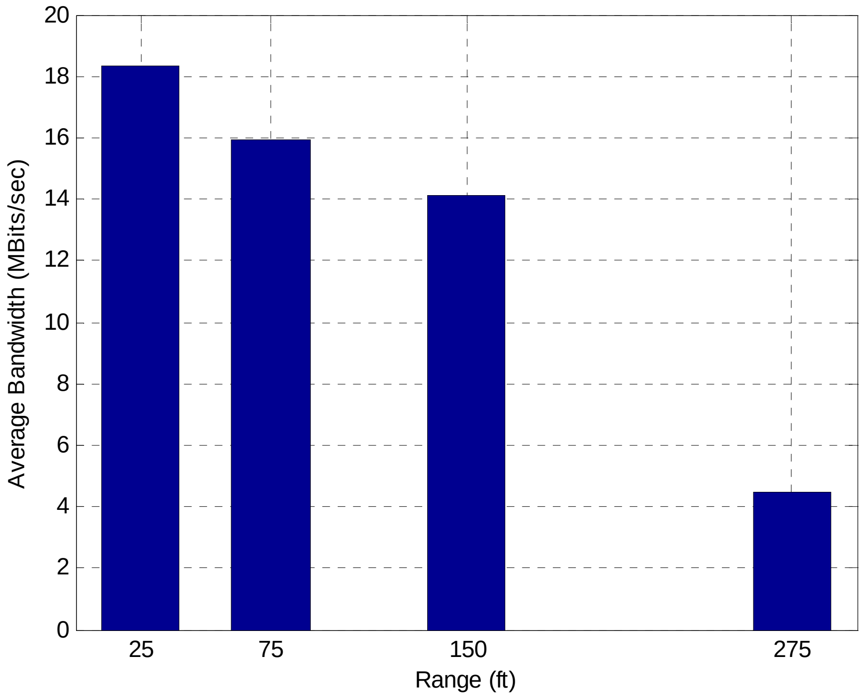


Figure 4-5: Bandwidth Variation for IEEE 802.11g Channel 11 (2.462 GHz) with Range

Similarly, these tests were conducted for both IEEE 802.11a and g protocols in the indoor environment. The test nodes were placed at a distance of 25 ft. Figure 4.6 shows the bandwidth measurement across trials. These results indicate that the performance of IEEE 802.11g is better than IEEE 802.11a in an indoor environment. One of the reasons is that IEEE 802.11a uses the 5 GHz frequency. This frequency is easily obstructed by materials such as walls, metal, cabins, et cetera.

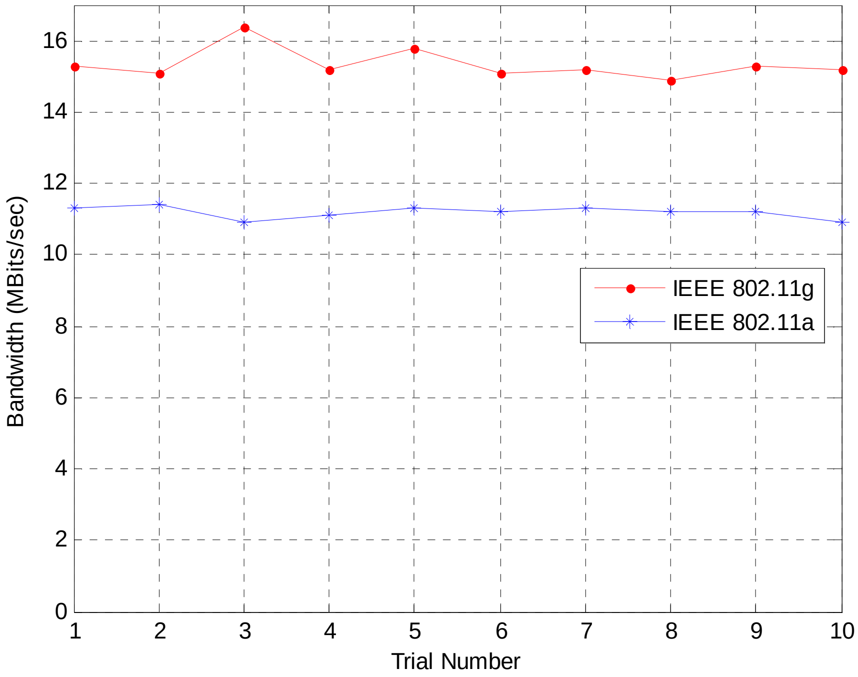


Figure 4-6: Bandwidth Measurement for IEEE 802.11a and g

Tcpdump was used to capture all the packets that were transmitted for the test run at each range, and then saved them within a capture file. *Tcptrace* was used to read this capture file and to obtain files that can be plotted. Bandwidth and Round Trip Time (RTT) plots were drawn using *jPlot*. The performance statistics were tabulated and shown in Tables 4.1 and 4.2 for frequency channels 1 and 11. Both of the channels showed similar performance with little deviation.

Range (ft)	Packets Sent	Avg. Packets/sec	Avg. Packet Size (Bytes)	Bytes Sent	Throughput (Mbit/sec)
25	48469	2418.635	1018	49359314	19.704
75	47963	2393.62	1004	48163206	19.229
150	46171	2303.427	983	45389494	18.116
275	12190	607.107	962	584507	4.676

Table 4-1: Throughput Performance of IEEE 802.11g Channel 1 with Range

Range (ft)	Packets Sent	Avg. Packets/sec	Avg. Packet Size (Bytes)	Bytes Sent	Throughput (Mbit/sec)
25	47645	2378.481	1023	48765858	19.475
75	41168	2053.742	1023	42128840	16.813
150	36760	1831.962	1023	37635692	15.005

Table 4-2: Throughput Performance of IEEE 802.11g Channel 11 with Range

The Figures 4.7 through 4.20 show the throughput and RTT for both channels 1 and 11 at each range tested. In the throughput plots the yellow dots represent instantaneous throughput, defined as the size of the segment seen divided by the time since the last segment was seen. The blue line tracks the average throughput of the connection up to that point for the lifetime of the connection (total bytes seen/total seconds so far). The red line tracks the throughput seen from the last few samples, calculated as the average of *N* previous yellow dots. By default the line tracks the past 10 samples (*N*=10). RTT is measured as the time a packet takes to reach the receiver and return. The X and Y axes represents the time span of the test performed (20 sec) and the roundtrip time of the packets at each instant respectively. The performance of the network was consistent throughout the test (Figures 4.7 to 4.12, and Figure 4.15 to 4.20). As the distance between the nodes increased, RTT increased (Figure 4.13), causing degradation in the throughput shown in Figure 4.14. The graphs indicate a consistent throughput performance up to a range of 150 ft.

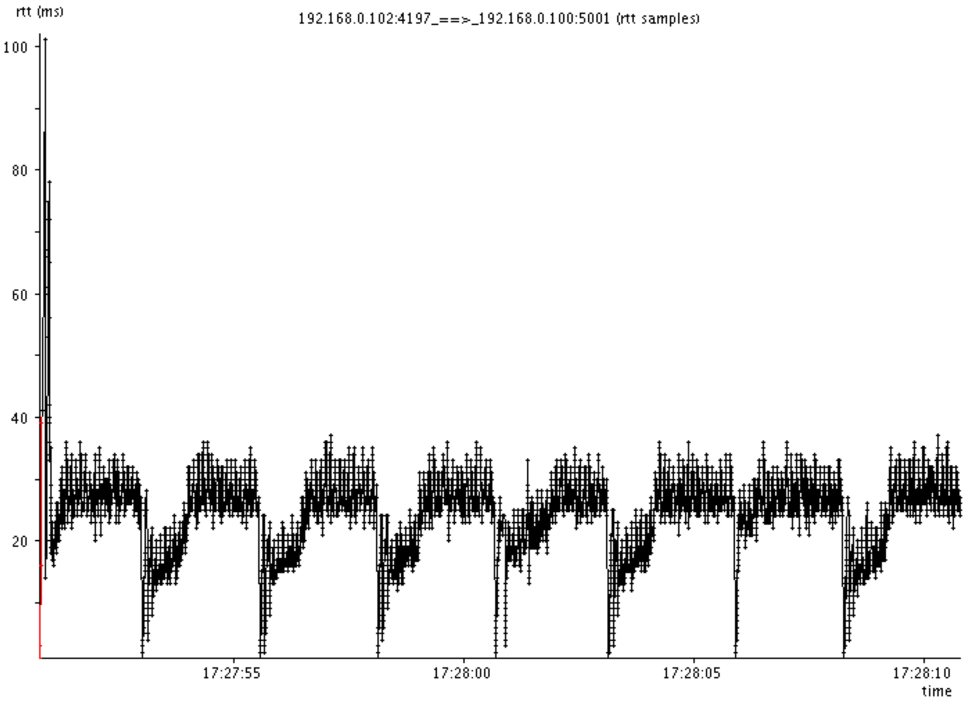


Figure 4-7: RTT Plot for Channel 1 at 25 ft

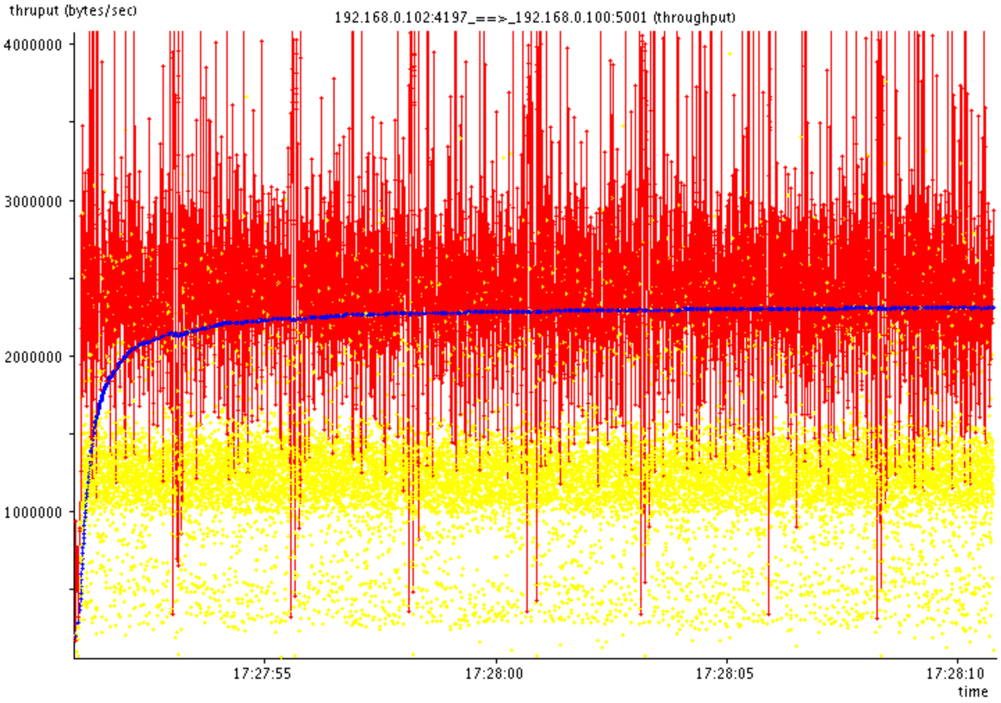


Figure 4-8: Throughput Plot for Channel 1 at 25 ft

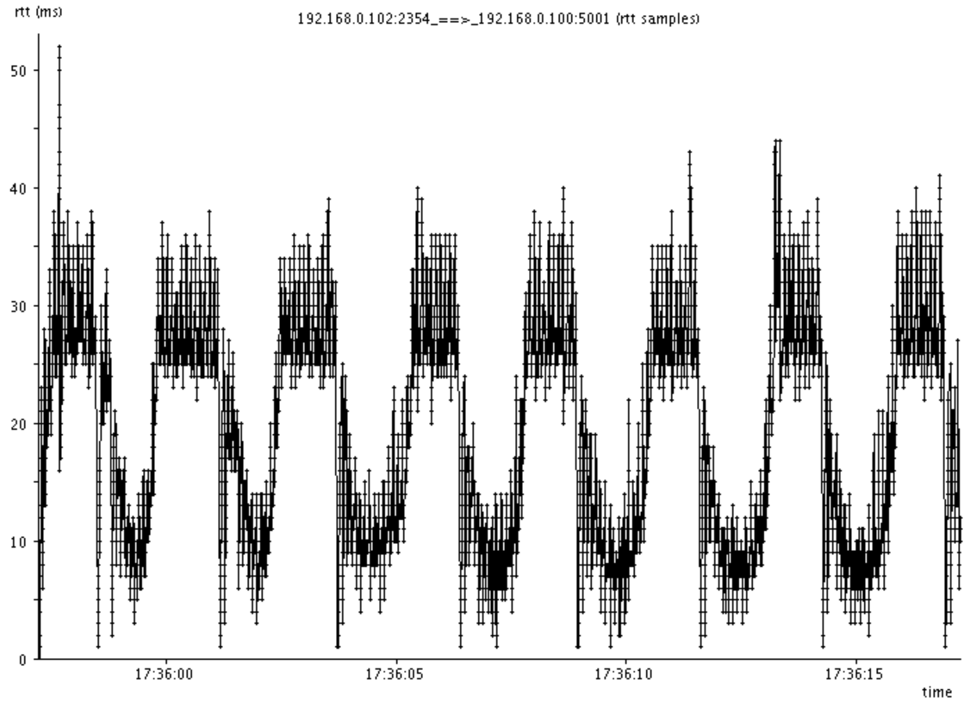


Figure 4-9: RTT Plot for Channel 1 at 75 ft

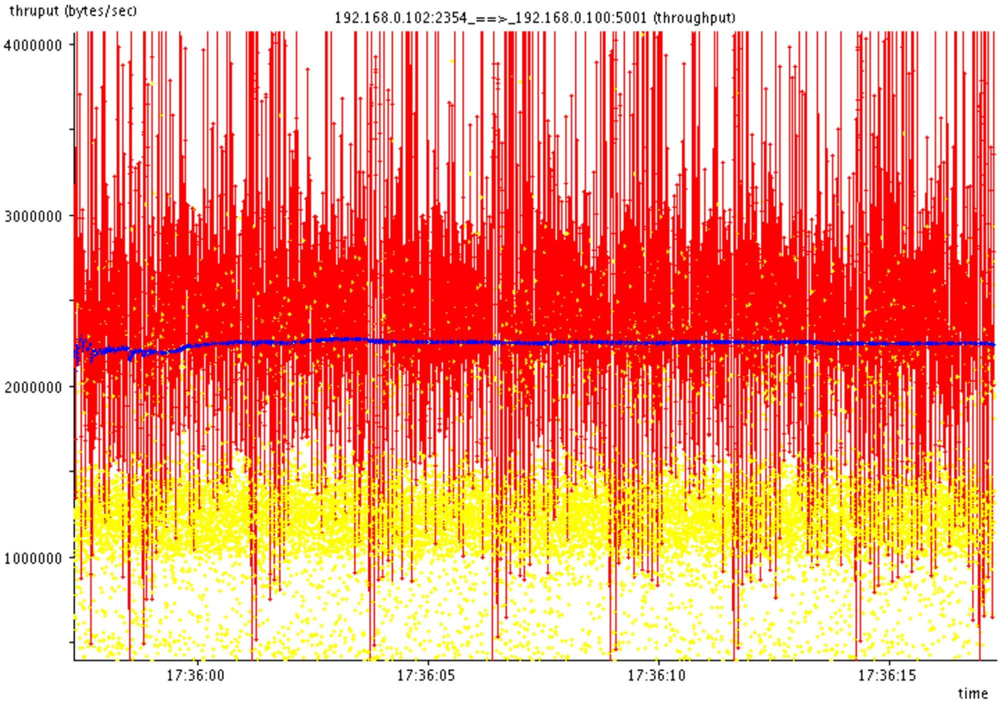


Figure 4-10: Throughput Plot for Channel 1 at 75 ft

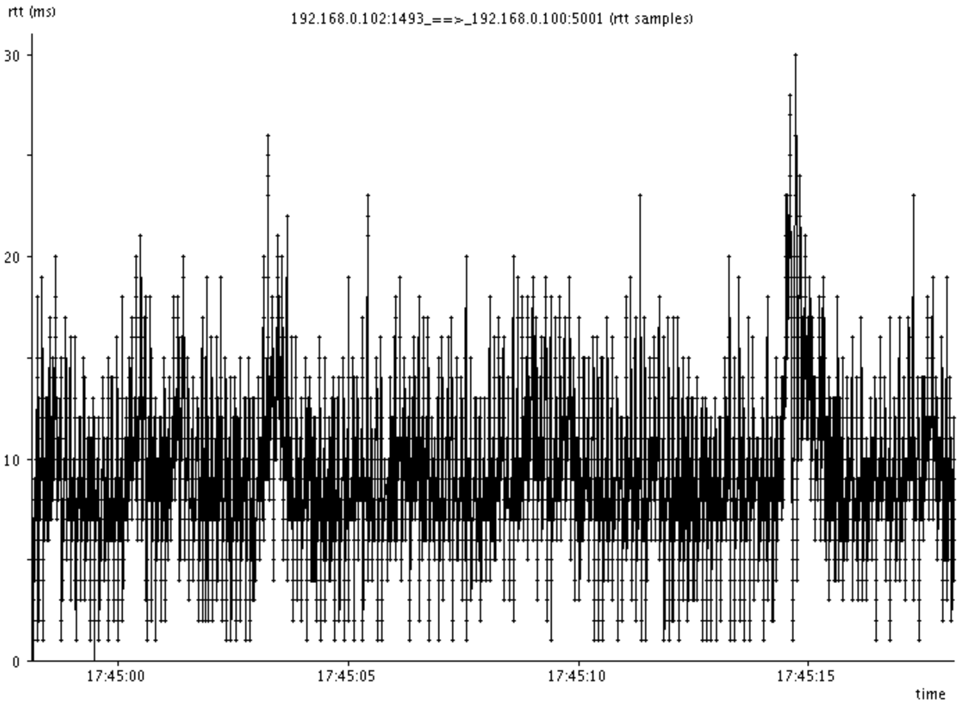


Figure 4-11: RTT Plot for Channel 1 at 150 ft

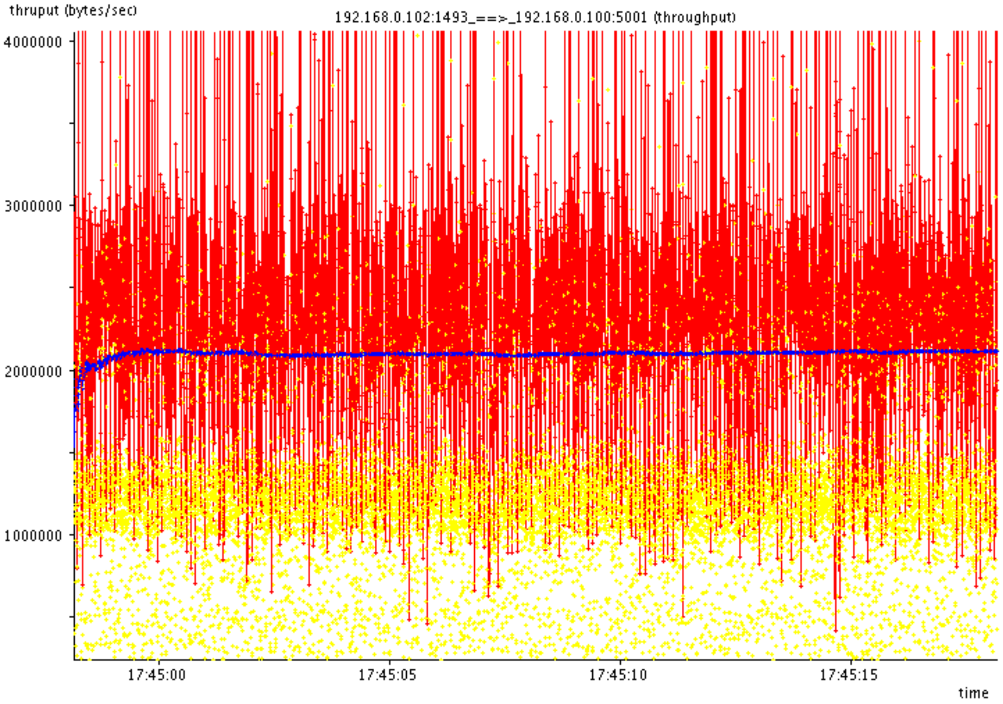


Figure 4-12: Throughput Plot for Channel 1 at 150 ft

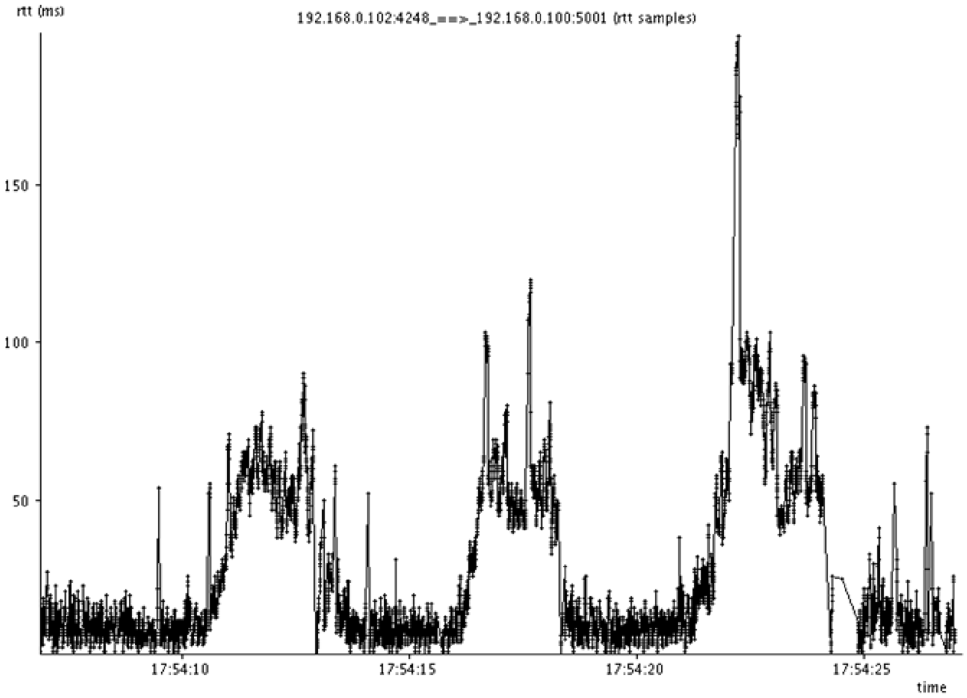


Figure 4-13: RTT Plot for Channel 1 at 275 ft

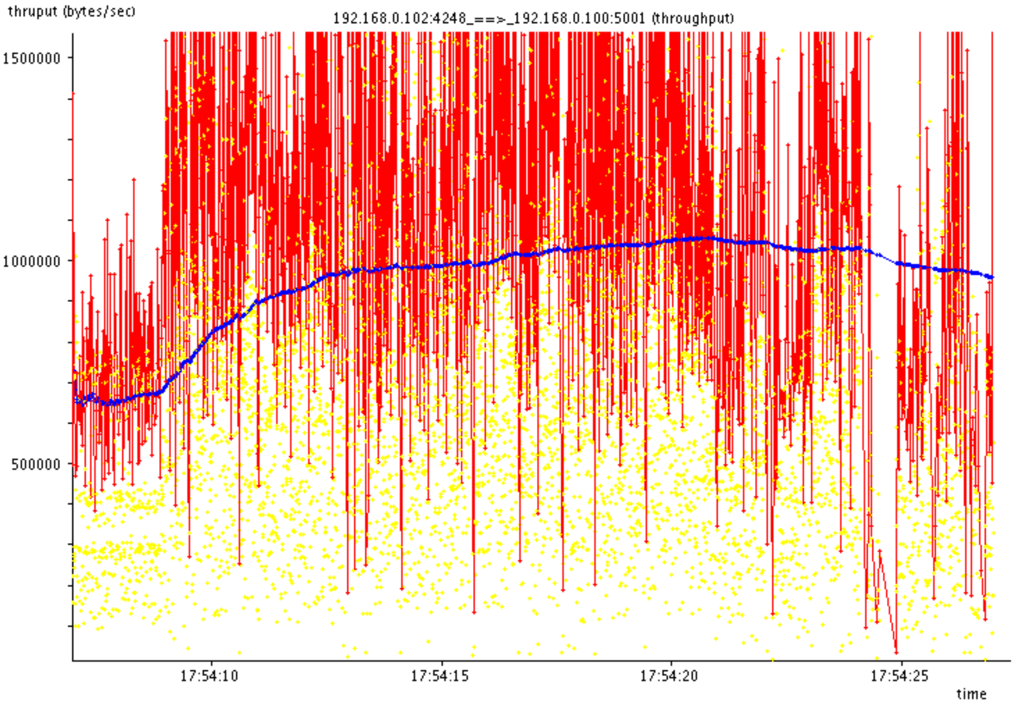


Figure 4-14:Throughput Plot for Channel 1 at 275 ft

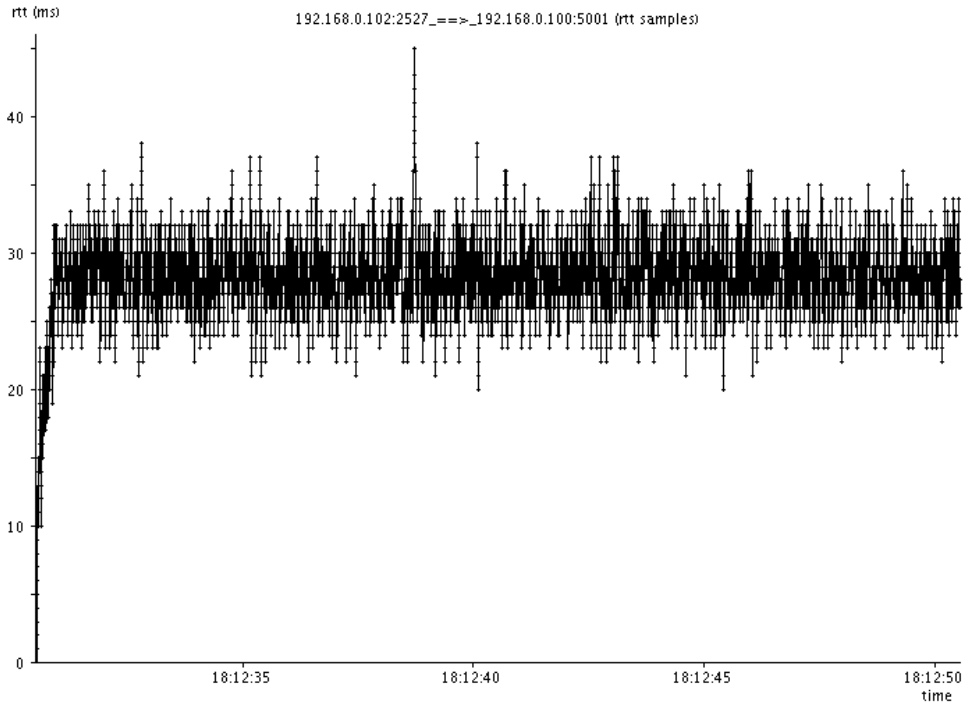


Figure 4-15: RTT Plot for Channel 11 at 25 ft

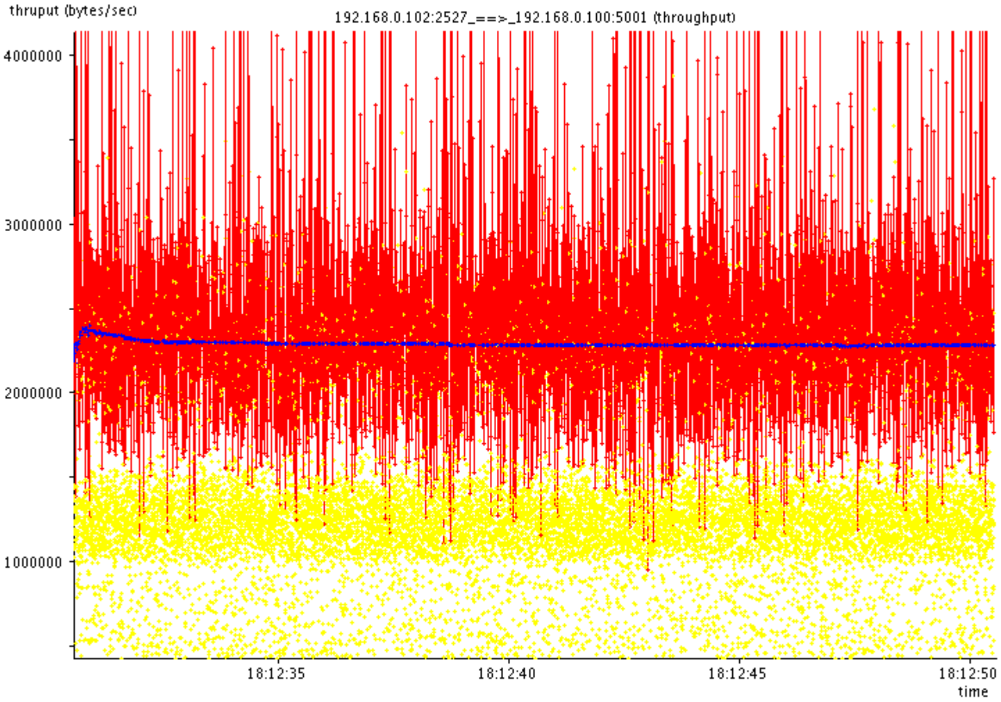


Figure 4-16: Throughput Plot for Channel 11 at 25 ft

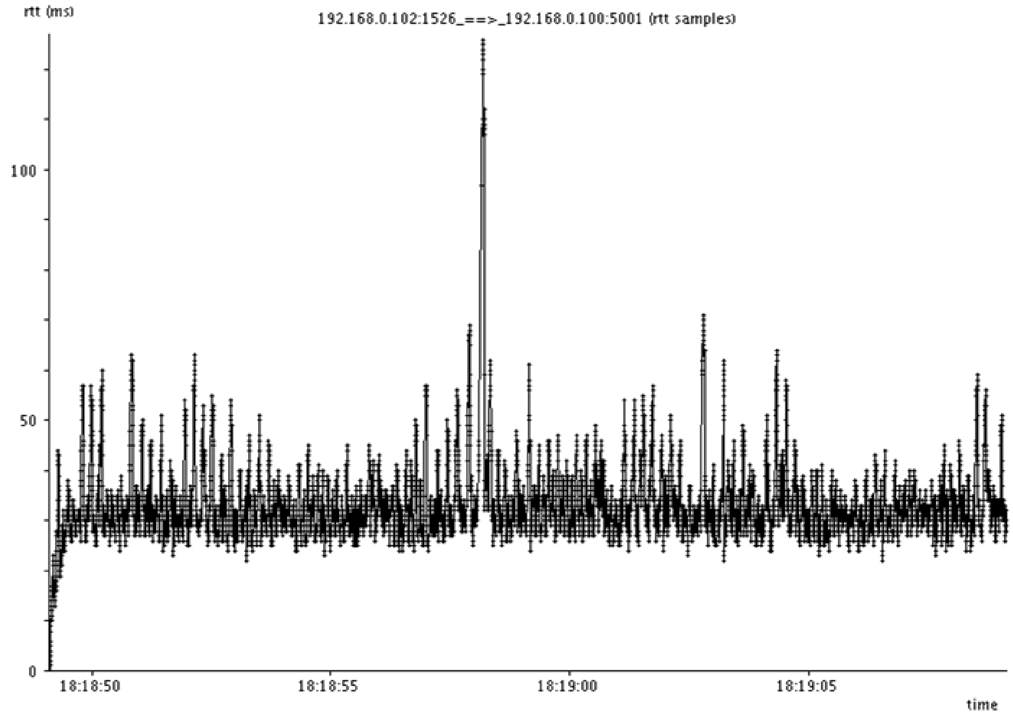


Figure 4-17: RTT Plot for Channel 11 at 75 ft

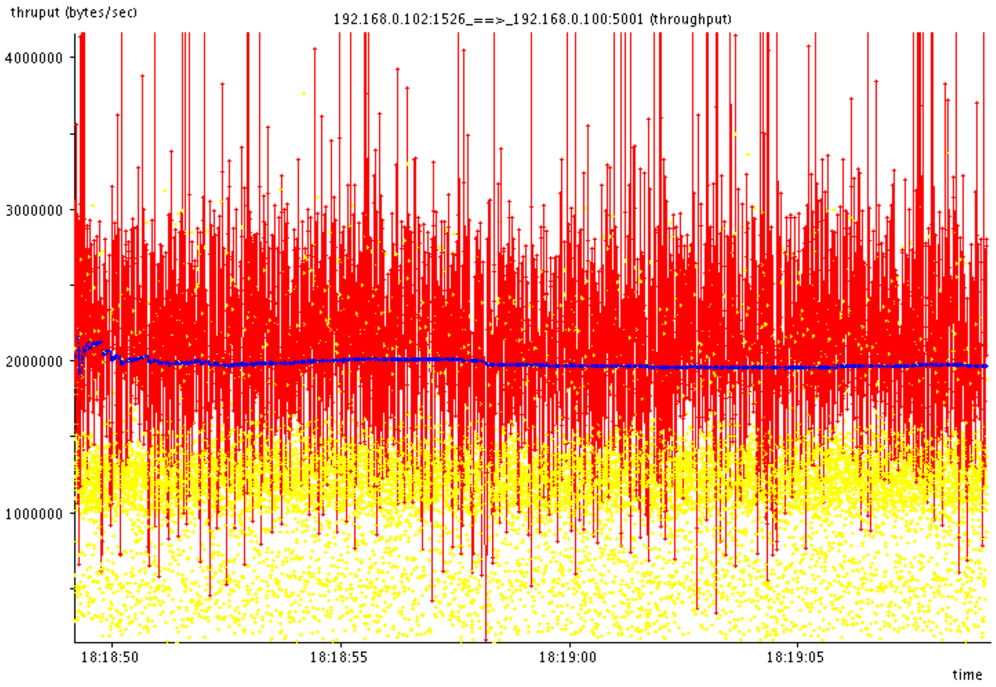


Figure 4-18: Throughput Plot for Channel 11 at 75 ft

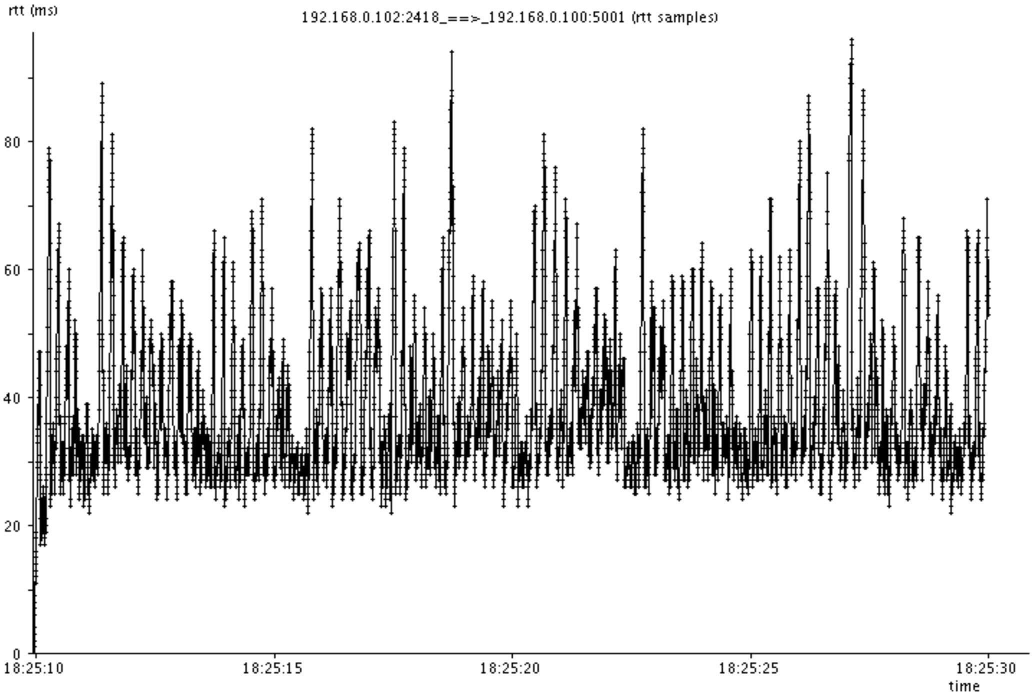


Figure 4-19: RTT Plot for Channel 11 at 150 ft

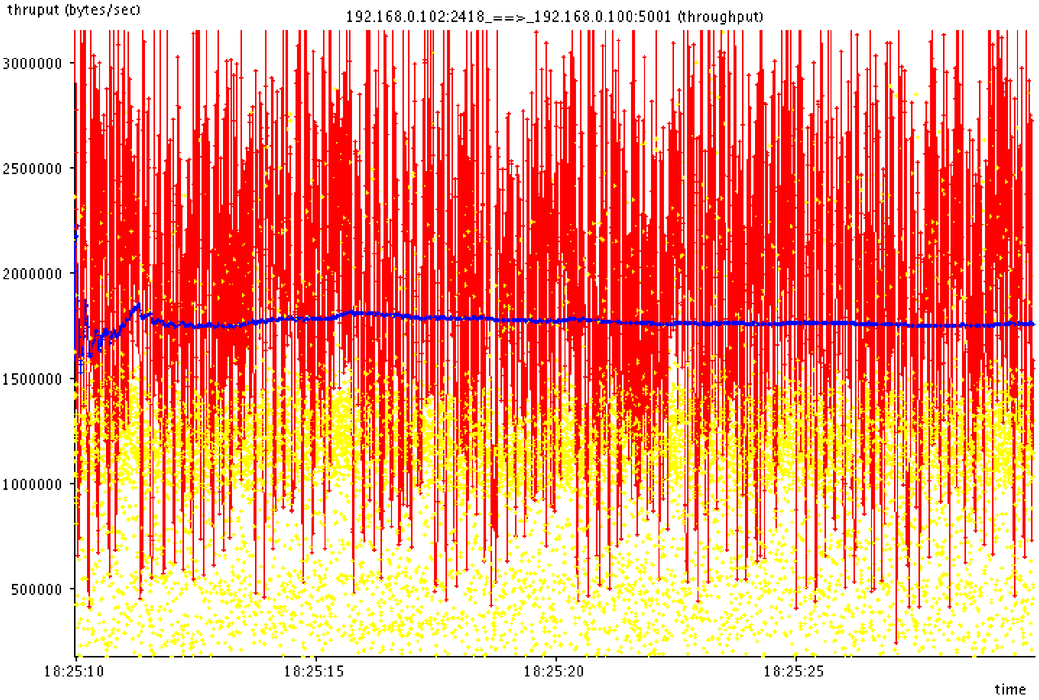


Figure 4-20: Throughput Plot for Channel 11 at 150 ft

As the range is increased between the two nodes the performance degrades. This is because of packet losses and retransmissions. The network performance was stable to a range of 150 ft, and offered a consistently high data rate of 15 Mbps. The inconsistency in the RTT plot at 275 ft (Figure 4.13) is because multiple retransmissions occurred due to the data losses and the fading of the wireless signal. The performance of IEEE 802.11a decreases drastically with range because of the fading of the high frequency signal. IEEE 802.11g performs better in environments surrounded by obstacles and where there is no direct line of sight. Another advantage with IEEE 802.11g over IEEE 802.11a is the cost of the equipment, so IEEE 802.11g was chosen for the future experiments.

4.2. Heterogeneous Network

In earlier sections, the research conducted on the implementation of wireless technologies for essential applications on an aircraft was addressed. Most of this research has been focused on the evaluation of wireless standards developed for unlicensed bands; for example, the 900 MHz, 2.4 GHz and 5 GHz ISM and UNII bands. Well known wireless standards operating within these bands are Bluetooth, ZigBee, and WiFi. Also, there are some products being used within the aircraft which use spread spectrum technologies. Evaluation of WiFi protocols interoperability with other wireless standards operating within the same frequency band is very important.

There are many low data rate applications within an aircraft. For some of these applications wireless technology has already been implemented. High speed wireless protocols could be overkill for low data rate applications. It is important to consider a low data rate protocol for some basic evaluation of its interoperability with WiFi. It is the IEEE 802.15.4 specification widely used within wireless sensor networks. ZigBee supports a data rate of 250 Kbps and has an indoor range of up to 300 feet. It can support a network of 60,000 nodes and different network topologies such as star, tree, mesh, etc. Mesh topologies have features like self-forming capabilities, which means the nodes are automatically configured into a network, and new paths are automatically selected when needed.

Figure 4.21 shows the 2.4 GHz frequency band with a comparison of WiFi and ZigBee standards. It can be observed that the power requirement for ZigBee is less than the WiFi standard. WiFi has three non-overlapping channels, and ZigBee has 16 channels within the 2.4 GHz frequency band. ZigBee uses 5 MHz band channels to support a data rate of 250 Kbps. WiFi uses 22 MHz channels and supports up to 54 Mbps (up to 11 Mbps for IEEE 802.11b). Whenever there is a need for simultaneous usage of both networks, care should be taken to use different transmission channels.

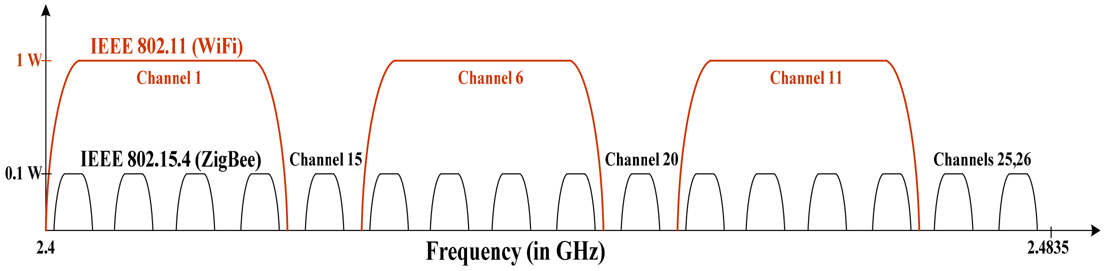


Figure 4-21: Overview of WiFi and ZigBee Channels in the 2.4 GHz Frequency Band

Analysis of the ZigBee network within an aircraft environment has been done using an XBee Professional development kit developed by MaxStream. Figure 4.22 shows a RS-232 development board with an XBee module.

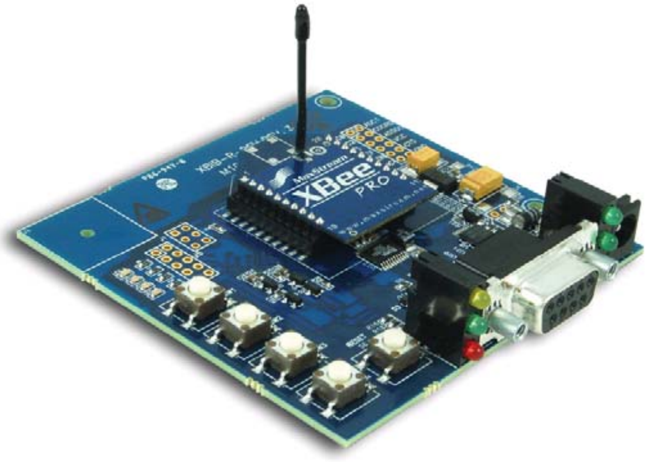


Figure 4-22: XBee Pro Development Board

Different I/O parameters, like baud rate, flow control, source and destination addresses within the modules, were configured using the X-CTU software. Two nodes were configured for communications using: 9,600 baud rate, 8 data bits, no parity, 1 stop bit (8-N-1), and no flow control. The nodes were given unique host and destination addresses. The USB development board was connected to the laptop and the RS-232 development board was connected to a serial loopback adapter. Figure 4.23 shows the test setup on the Cessna 172 airframe at our Flight Research Laboratory.

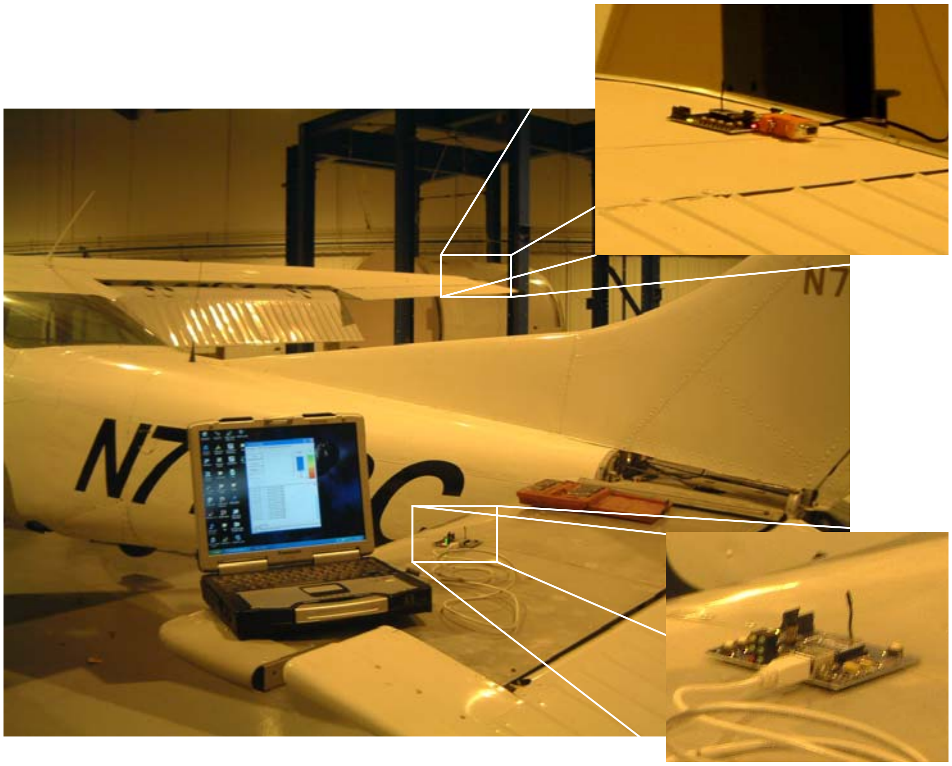


Figure 4-23: Test Setup of ZigBee Modems on an Airframe

The nodes were tested at different locations within the airframe. A WiFi network was already present in the hanger during the entire experiment.

A 32 byte message was chosen from X-CTU. Data transmissions were conducted for a considerable amount of time over each distance. Statistics such as the data received, the signal strength, and the percentage of good data packets transmitted can be obtained from X-CTU. Results show that there was insignificant loss of data at any location on the airframe even though there was no line of sight from some positions. It was observed that out of 135 packets transmitted there were only 5 bad packets, and that the signal strength was always very good. It was observed that there would be no interference between the WiFi modules and the ZigBee modems if both of them were operating on different frequency channels.

These ZigBee modules were also evaluated with a GPS 15L module from Garmin. Figure 4.24 shows the experimental setup on the bench. The modems were configured for 4,800 Baud, 1 stop bit (8-N-1), and no flow control. The RS-232 development board was connected to the GPS receiver, and the USB board was connected to the laptop. GPS Express 3.2 was used to receive the GPS data.

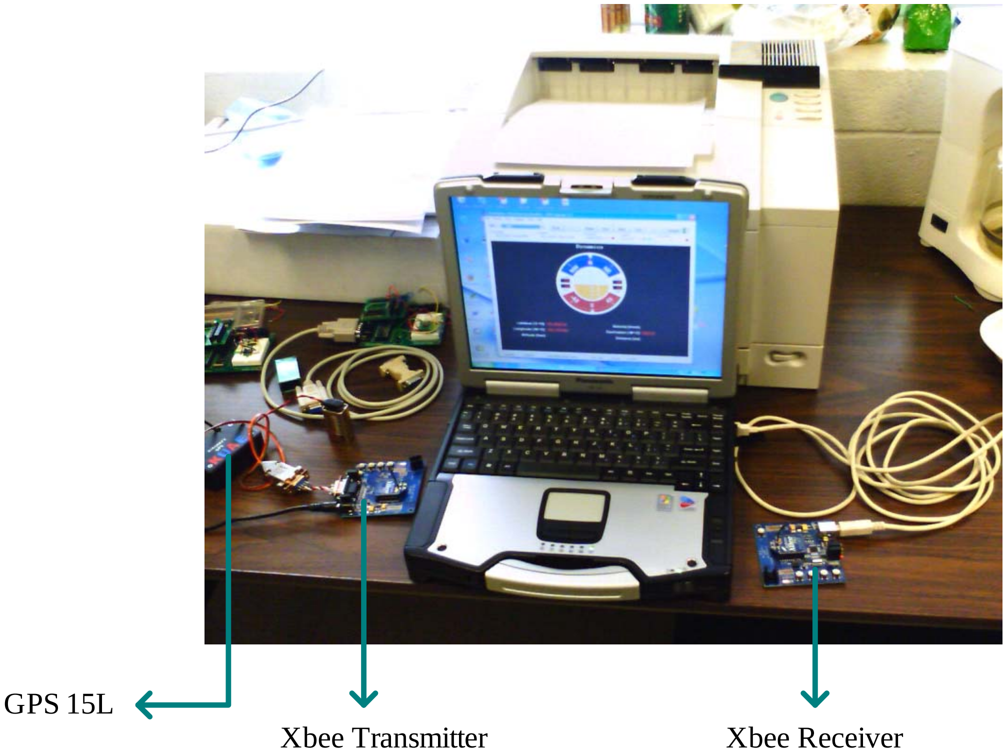


Figure 4-24: Test Setup of the ZigBee Based Wireless GPS Communications

5. Evaluation of the Two Node Wireless Avionics Network

The wireless network performance tests were accomplished using network analysis tools such as *IPerf* and *TCPdump.* They showed that IEEE 802.11g supports a high data rate (14 Mbps) even at a range of 150 feet. This is sufficient for most of the data communication requirements for a general aviation aircraft. The previous experiments were to measure the wireless link performance where there were no real flight instruments involved. It is important to evaluate the performance of the wireless network with sensors which are normally connected using RS-232, RS-485, or ARINC 429 interfaces. Also, it is important to measure the availability of the wireless link in different operational conditions. This chapter describes the development of a two node wireless avionics network between the AHRS and the cockpit display unit. Significant testing has been done on the ground before the flight test of the network was accomplished for the real time performance analysis. The ground test and flight test results are given in this chapter.

5.1. Development of the Two Node Network

To determine the accuracy and availability of the wireless avionics network it is important to test the avionics network under different test conditions. A two node network has been developed between the cockpit display unit and the wireless AHRS unit. Figure 5.1 shows the architectural view of the two node network. The network was configured as follows.

- Mode: Ad-Hoc
- Protocol: IEEE 802.11g
- Channel: 11 (2.462 GHz)
- SSID: ADMRC
- Authentication: Open
- Key: WEP 64 bit

Both the nodes were assigned IP addresses.

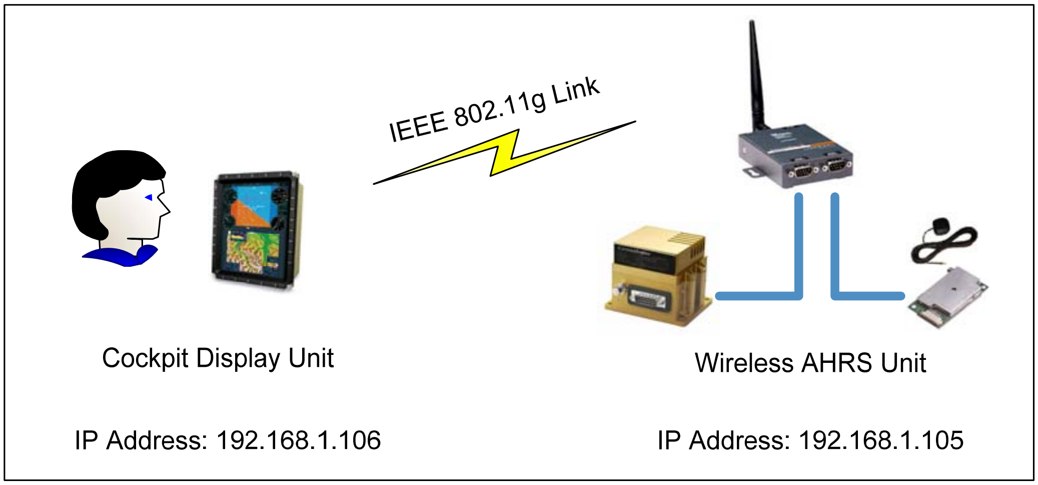
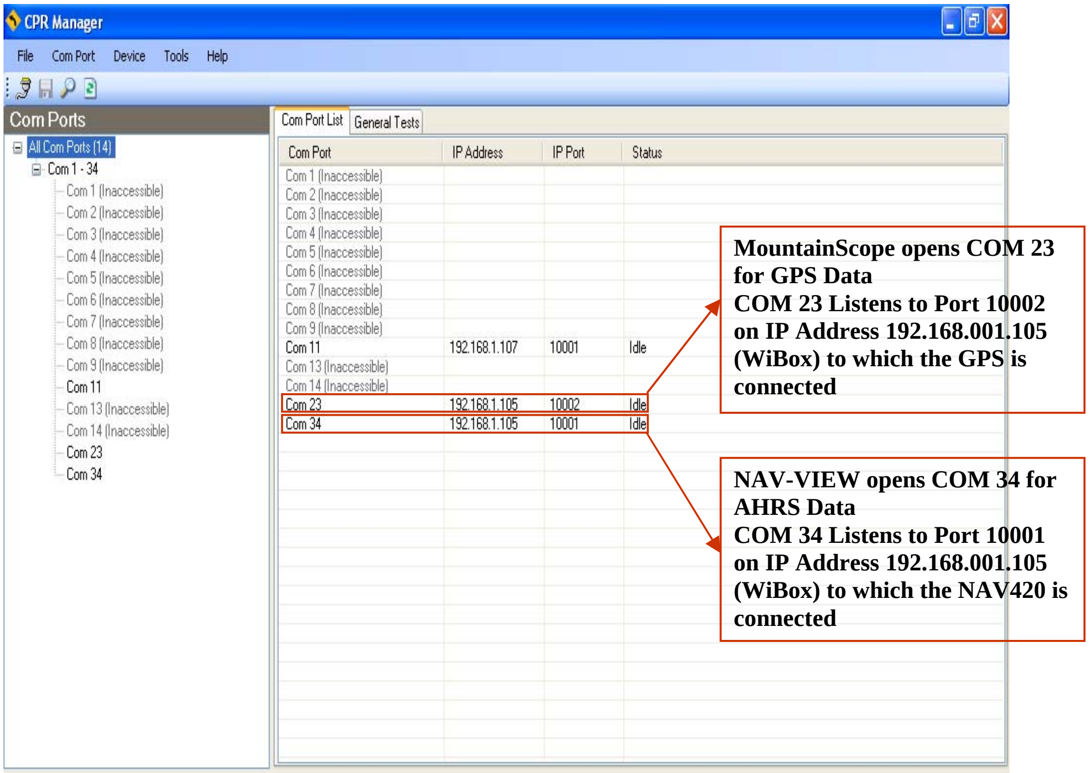


Figure 5-1: Schematic of the Two Node Wireless Avionics Network

Following standard practice, the NAV420 and GPS are connected to the flight computer and/or the primary flight display using an RS-232 interface. Moving map software and the navigational display software read the data through the physical communication (COM) ports of the system. In the wireless network, the data is transmitted between the network interface cards of the nodes. Since the software installed in the Cockpit Display Unit (CDU) are capable of reading the data from the sensors via the systems COM ports, there was a requirement to transfer the data coming to the network interface card to the COM ports. This was achieved by software provided by Lantronix® known as Com Port Redirector (CPR). Using CPR, two virtual COM ports (COM 23 and 34) were configured on the CDU. These COM ports are redirected on the wireless network to the serial ports of the WiBox in the Wireless AHRS unit to which the NAV420 was connected. COM 23 was configured to port "10002" of the WiBox with the following specifications: 9,600 baud rate, 8 data bits, no parity, and one stop bit suitable for reading GPS data. Similarly, COM 34 was configured to the port "10001" of the WiBox with the specification: 38,400 baud rate, 8 data bits, no parity and one stop bit (which is the default setting for NAV420). Table 5.1 summarizes the virtual COM port settings on the CDU. Figure 5.2 shows the CPR window with COM 23 and 34 configured to the IP address 192.168.1.105 that belongs to the WiBox in the network.

Virtual COM Port on CDU	Sensor Type	Serial Port on WiBox	Configuration
23	GPS	10002	9600 Baud, 8-N-1
34	NAV420	10001	38400 Baud, 8-N-1

Table 5-1: Virtual Port Configuration on CDU



Com Port	IP Address	IP Port	Status
Com 1 (Inaccessible)			
Com 2 (Inaccessible)			
Com 3 (Inaccessible)			
Com 4 (Inaccessible)			
Com 5 (Inaccessible)			
Com 6 (Inaccessible)			
Com 7 (Inaccessible)			
Com 8 (Inaccessible)			
Com 9 (Inaccessible)			
Com 11	192.168.1.107	10001	Idle
Com 13 (Inaccessible)			
Com 14 (Inaccessible)			
Com 23	192.168.1.105	10002	Idle
Com 34	192.168.1.105	10001	Idle

MountainScope opens COM 23 for GPS Data
COM 23 Listens to Port 10002 on IP Address 192.168.001.105 (WiBox) to which the GPS is connected

NAV-VIEW opens COM 34 for AHRS Data
COM 34 Listens to Port 10001 on IP Address 192.168.001.105 (WiBox) to which the NAV420 is connected

Figure 5-2: CPR Window Showing COM Ports 23 & 34 Configured with WiBox

In order to transmit the data from the wireless AHRS unit to the CDU, they have to be associated to the network “ADMRC”. MountainScope and NAV-VIEW were set to open COM ports 23 and 34, respectively, to receive the sensor data. Figure 5.3 shows the architectural view of the network in which the WiBox sends the data to the TCP/IP network and the CDU accesses the sensor data. The dotted line indicates the actual data communication link between the components.

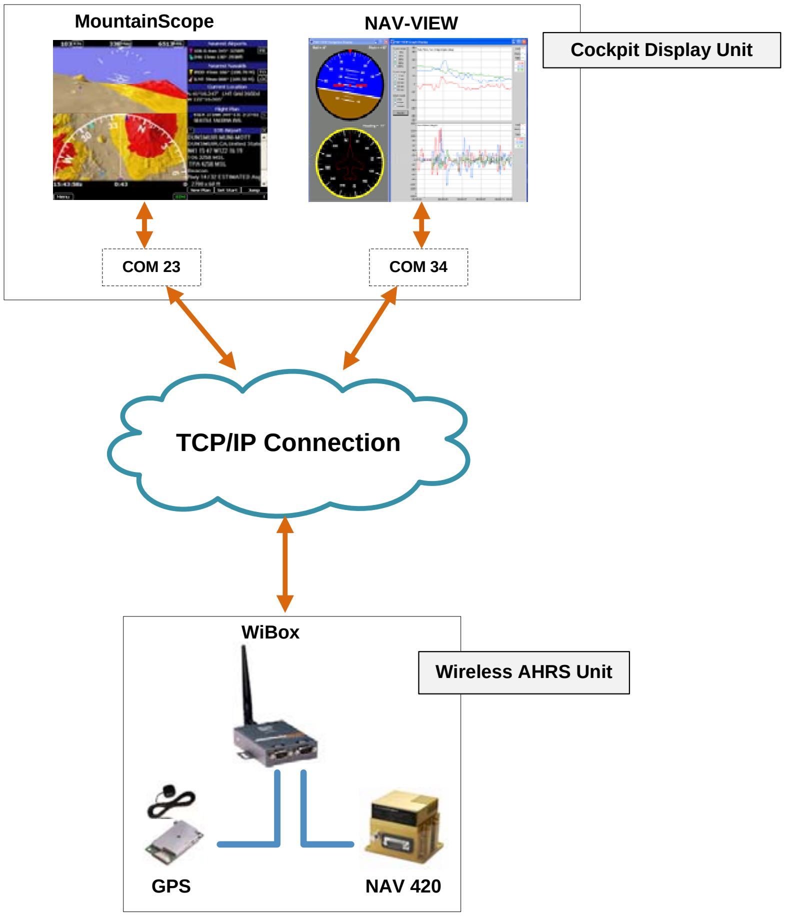
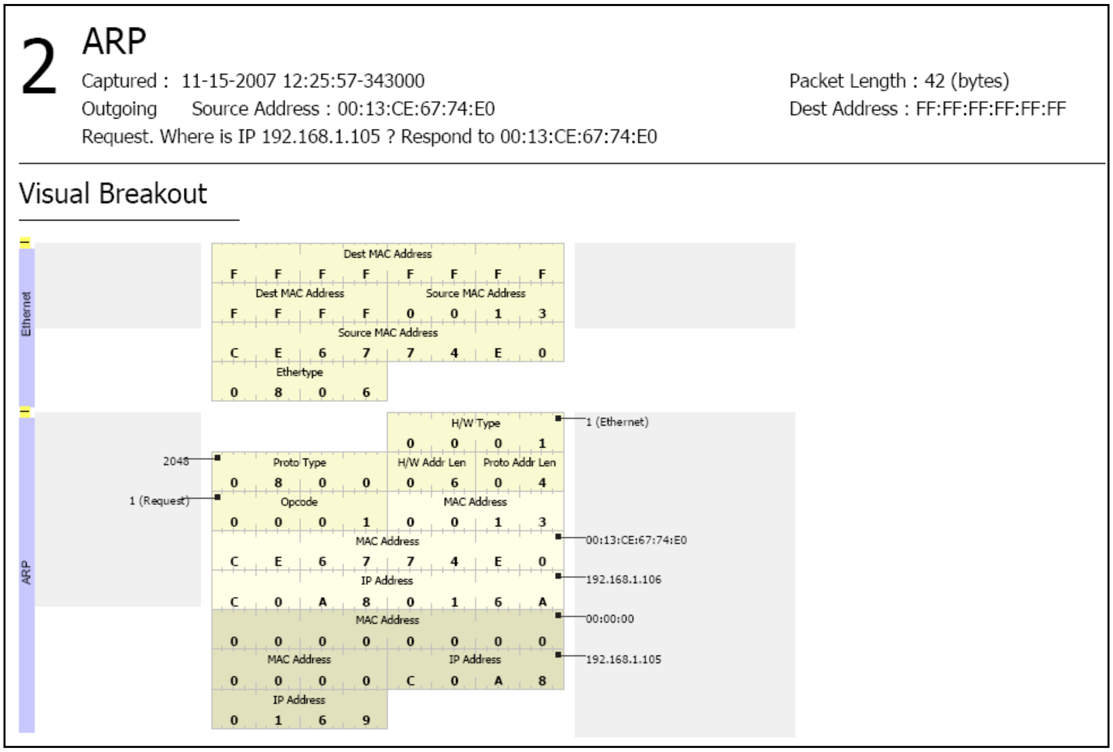


Figure 5-3: Architecture of the Two Node Wireless Avionics Network

When the software tries to access data from the COM ports, CDU (IP: 192.168.1.106, MAC: 00:13:CE:67:74:E0) sends an ARP (Address Resolution Protocol), which is a broadcast message, requesting the machine that has IP address 192.168.1.105 to respond, as shown in Figure 5.4. WiBox (MAC: 00:20:4A:96:63:DC) responds to the request by sending another ARP packet saying it has the IP 192.168.1.105, shown in Figure 5.5. During the ARP packet transmission they represent their MAC addresses. Then the WiBox sends a UDP (Figure 5.6) packet with its IP address destined to the IP address of the CDU. After that, the CDU sends a SYN (Synchronization) packet (Figure 5.7), which is a TCP packet confirming details such as: Maximum Segment Size (MSS), sequence number, window size, port numbers for communication (1557 for CDU, 10001 for WiBox), etc. The handshaking has been captured using *IP Sniffer*, and the captured file analyzed using *Unsniffer Network Analyzer*. Figures 5.4 through 5.7 show the visual breakout diagrams of different protocols involved in the connection formation for the network.



2 ARP

Captured : 11-15-2007 12:25:57-343000 Packet Length : 42 (bytes)

Outgoing Source Address : 00:13:CE:67:74:E0 Dest Address : FF:FF:FF:FF:FF:FF

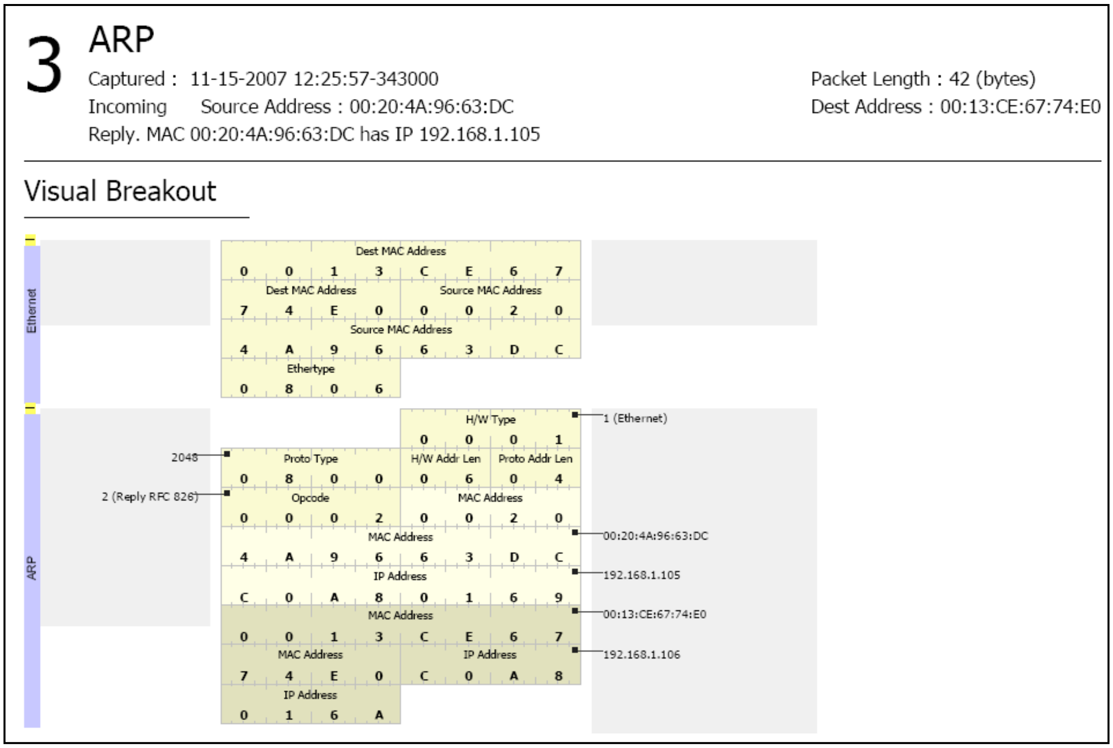
Request. Where is IP 192.168.1.105 ? Respond to 00:13:CE:67:74:E0

Visual Breakout

```
Ethernet
                Dest MAC Address
      F   F   F   F   F   F   F   F
    Dest MAC Address   Source MAC Address
      F   F   F   F   0   0   1   3
                Source MAC Address
      C   E   6   7   7   4   E   0
        Ethertype
      0   8   0   6

ARP
                          H/W Type
                      0   0   0   1          1 (Ethernet)
2048        Proto Type     H/W Addr Len  Proto Addr Len
      0   8   0   0   0   6   0   4
1 (Request)  Opcode         MAC Address
      0   0   0   1   0   0   1   3
                  MAC Address
      C   E   6   7   7   4   E   0          00:13:CE:67:74:E0
                  IP Address
      C   0   A   8   0   1   6   A          192.168.1.106
                  MAC Address
      0   0   0   0   0   0   0   0          00:00:00
       MAC Address        IP Address
      0   0   0   0   C   0   A   8          192.168.1.105
       IP Address
      0   1   6   9
```

Figure 5-4: ARP Broadcast Message from the CDU Requesting IP 192.168.1.105 to Respond



3 ARP

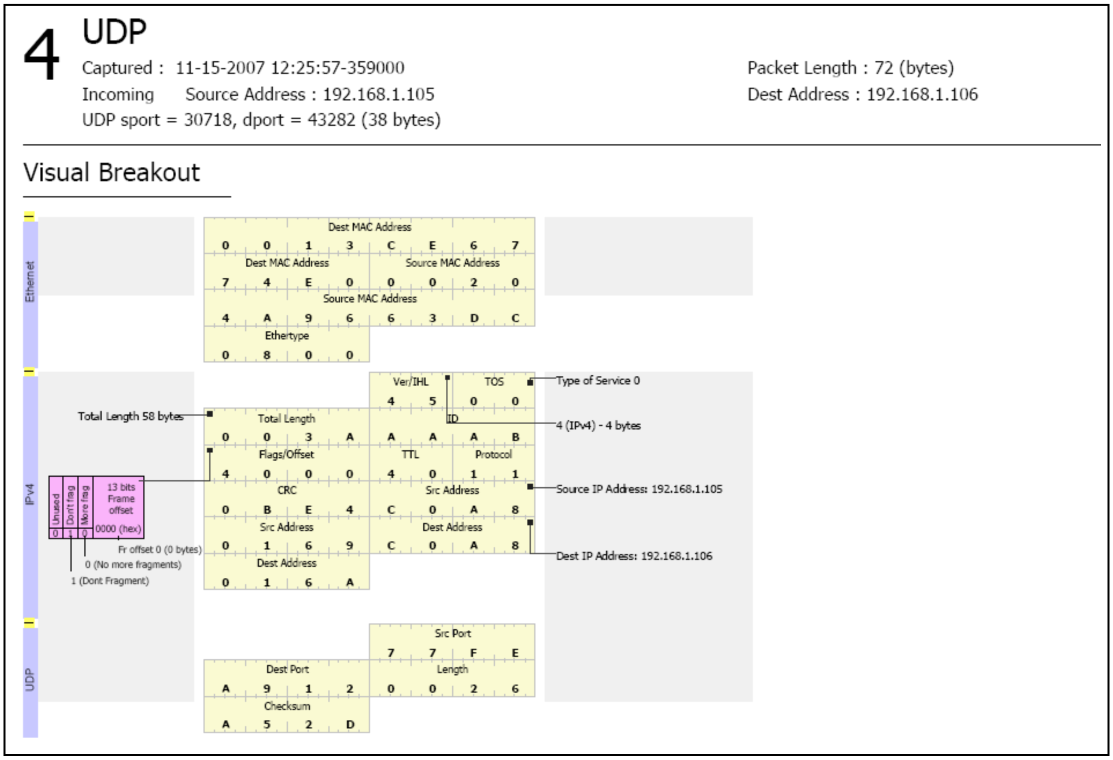
Captured : 11-15-2007 12:25:57-343000 Packet Length : 42 (bytes)

Incoming Source Address : 00:20:4A:96:63:DC Dest Address : 00:13:CE:67:74:E0

Reply. MAC 00:20:4A:96:63:DC has IP 192.168.1.105

Visual Breakout

Figure 5-5: ARP Response Message from WiBox



4 UDP

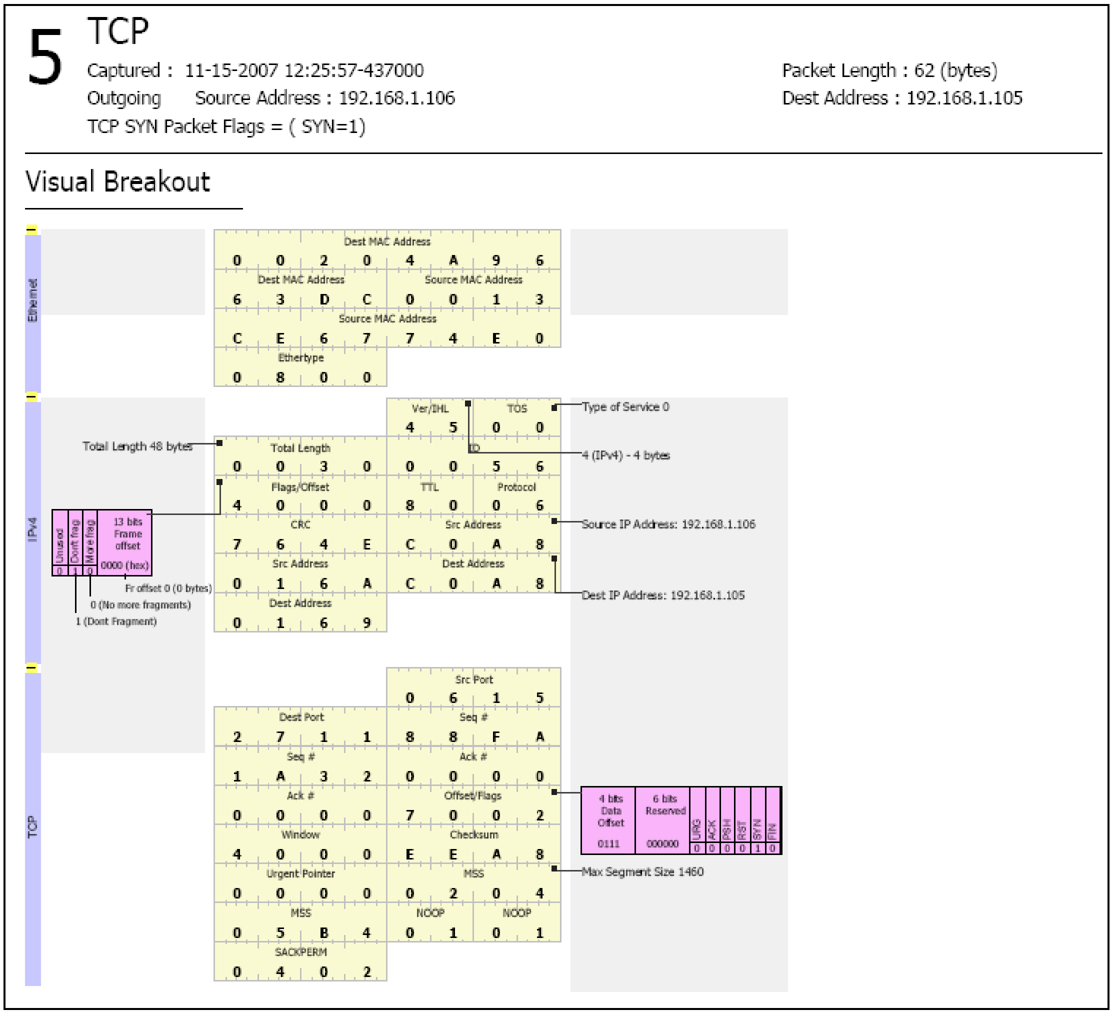
Captured : 11-15-2007 12:25:57-359000 Packet Length : 72 (bytes)

Incoming Source Address : 192.168.1.105 Dest Address : 192.168.1.106

UDP sport = 30718, dport = 43282 (38 bytes)

Visual Breakout

Figure 5-6: UDP Packet from WiBox to CDU



5 TCP

Captured : 11-15-2007 12:25:57-437000
Outgoing Source Address : 192.168.1.106
TCP SYN Packet Flags = (SYN=1)

Packet Length : 62 (bytes)
Dest Address : 192.168.1.105

Visual Breakout

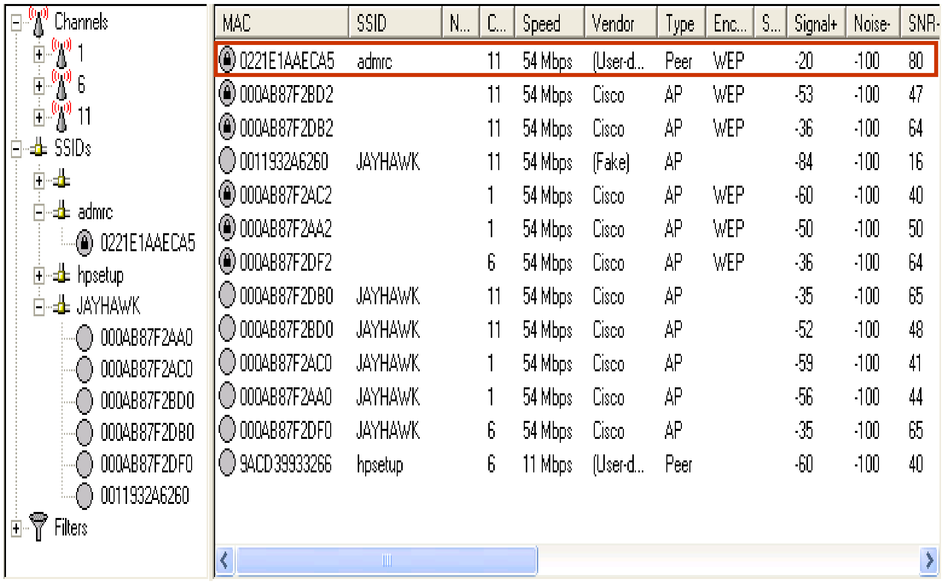
Figure 5-7: TCP SYN Packet from CDU to WiBox

Once the SYN packet has been sent to the WiBox, the CDU gets an acknowledgement (ACK) packet from the WiBox and data transmission will be started between these two nodes. The entire process takes a few milliseconds. Different network analysis tools were used for troubleshooting and to understand the data transmission over the wireless link.

5.2. Ground Test

The wireless avionics network has been evaluated under different test conditions on the ground to determine the robustness of the link. WiFi is a very widespread technology that was adopted in a vast array of applications. Most of laptops and PDAs are equipped with IEEE 802.11b/g standard hardware. It is easy to find a wide variety of test conditions for the avionics network within any urban environment. It was interesting to learn how the avionics network performs on crowded frequency channels. The network was tested in environments with varying numbers of outside networks operating within the same frequency band. *NetStumbler* was used to scan the environment and to find how the signal strength was varying in different conditions.

The avionics network was configured to channel 11 for the entire test. It was observed that the Signal to Noise Ratio (SNR) of the avionics network was very good when few networks were using the same frequency. The average signal strength was -30 dBm peaking to -20 dBm in some time periods. The network was able to support a data rate of 54 Mbps. Figure 5.8 shows the number of networks located in the vicinity, operating channel, and signal strength, et cetera. using *NetStumbler*. Figure 5.9 shows the SNR plot of the wireless link with signal strength (dBm) on the Y-axis and time on the X-axis. When the test was repeated in the presence of 80 access points, out of which 30 were operating in channel 11, there was significant fluctuation in the signal strength, with an average value of -50 dBm. Figure 5.10 shows the access points present in the vicinity. Figure 5.11 shows the signal strength of the avionics network in the presence of multiple networks within the same RF channel.



MAC	SSID	N...	C...	Speed	Vendor	Type	Enc...	S...	Signal+	Noise-	SNR-
0221E1AAECA5	admrc		11	54 Mbps	(User-d...	Peer	WEP		-20	-100	80
000AB87F2BD2			11	54 Mbps	Cisco	AP	WEP		-53	-100	47
000AB87F2DB2			11	54 Mbps	Cisco	AP	WEP		-36	-100	64
0011932A6260	JAYHAWK		11	54 Mbps	(Fake)	AP			-84	-100	16
000AB87F2AC2			1	54 Mbps	Cisco	AP	WEP		-60	-100	40
000AB87F2AA2			1	54 Mbps	Cisco	AP	WEP		-50	-100	50
000AB87F2DF2			6	54 Mbps	Cisco	AP	WEP		-36	-100	64
000AB87F2DB0	JAYHAWK		11	54 Mbps	Cisco	AP			-35	-100	65
000AB87F2BD0	JAYHAWK		11	54 Mbps	Cisco	AP			-52	-100	48
000AB87F2AC0	JAYHAWK		1	54 Mbps	Cisco	AP			-59	-100	41
000AB87F2AA0	JAYHAWK		1	54 Mbps	Cisco	AP			-56	-100	44
000AB87F2DF0	JAYHAWK		6	54 Mbps	Cisco	AP			-35	-100	65
9ACD39933266	hpsetup		6	11 Mbps	(User-d...	Peer			-60	-100	40

Figure 5-8: NetStumbler User Interface showing 13 Access Points in the Vicinity

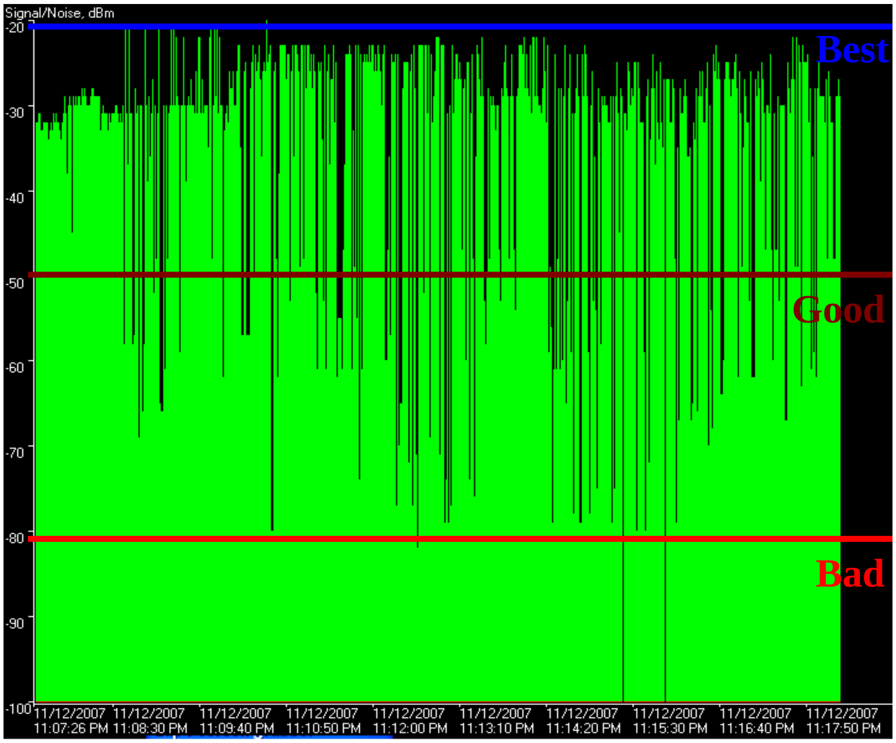
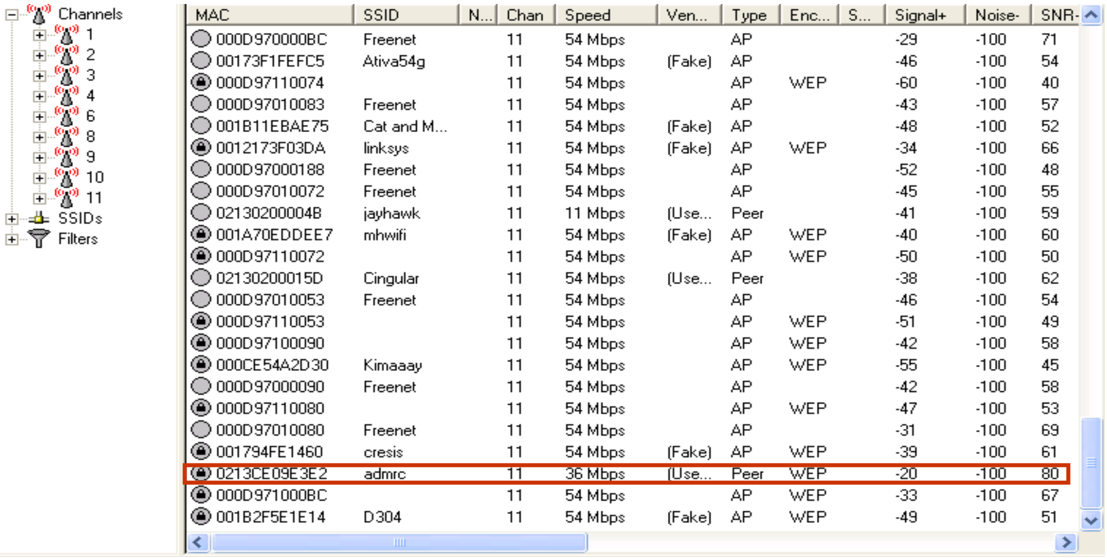


Figure 5-9: SNR Plot of the Wireless Avionics Network in the Presence of 13 Access Points



MAC	SSID	N...	Chan	Speed	Ven...	Type	Enc...	S...	Signal+	Noise-	SNR-
000D970000BC	Freenet		11	54 Mbps		AP			-29	-100	71
00173F1FEFC5	Ativa54g		11	54 Mbps	(Fake)	AP			-46	-100	54
000D97110074			11	54 Mbps		AP	WEP		-60	-100	40
000D97010083	Freenet		11	54 Mbps		AP			-43	-100	57
001B11EBAE75	Cat and M...		11	54 Mbps	(Fake)	AP			-48	-100	52
0012173F03DA	linksys		11	54 Mbps	(Fake)	AP	WEP		-34	-100	66
000D97000188	Freenet		11	54 Mbps		AP			-52	-100	48
000D97010072	Freenet		11	54 Mbps		AP			-45	-100	55
02130200004B	jayhawk		11	11 Mbps	(Use...	Peer			-41	-100	59
001A70EDDEE7	mhwifi		11	54 Mbps	(Fake)	AP	WEP		-40	-100	60
000D97110072			11	54 Mbps		AP	WEP		-50	-100	50
02130200015D	Cingular		11	54 Mbps	(Use...	Peer			-38	-100	62
000D97010053	Freenet		11	54 Mbps		AP			-46	-100	54
000D97110053			11	54 Mbps		AP	WEP		-51	-100	49
000D97100090			11	54 Mbps		AP	WEP		-42	-100	58
000CE54A2D30	Kimaaay		11	54 Mbps		AP	WEP		-55	-100	45
000D97000090	Freenet		11	54 Mbps		AP			-42	-100	58
000D97110080			11	54 Mbps		AP	WEP		-47	-100	53
000D97010080	Freenet		11	54 Mbps		AP			-31	-100	69
001794FE1460	cresis		11	54 Mbps	(Fake)	AP	WEP		-39	-100	61
0213CE09E3E2	admrc		11	36 Mbps	(Use...	Peer	WEP		-20	-100	80
000D971000BC			11	54 Mbps		AP	WEP		-33	-100	67
001B2F5E1E14	D304		11	54 Mbps	(Fake)	AP	WEP		-49	-100	51

Figure 5-10: NetStumbler User Interface showing Access Points in the Vicinity

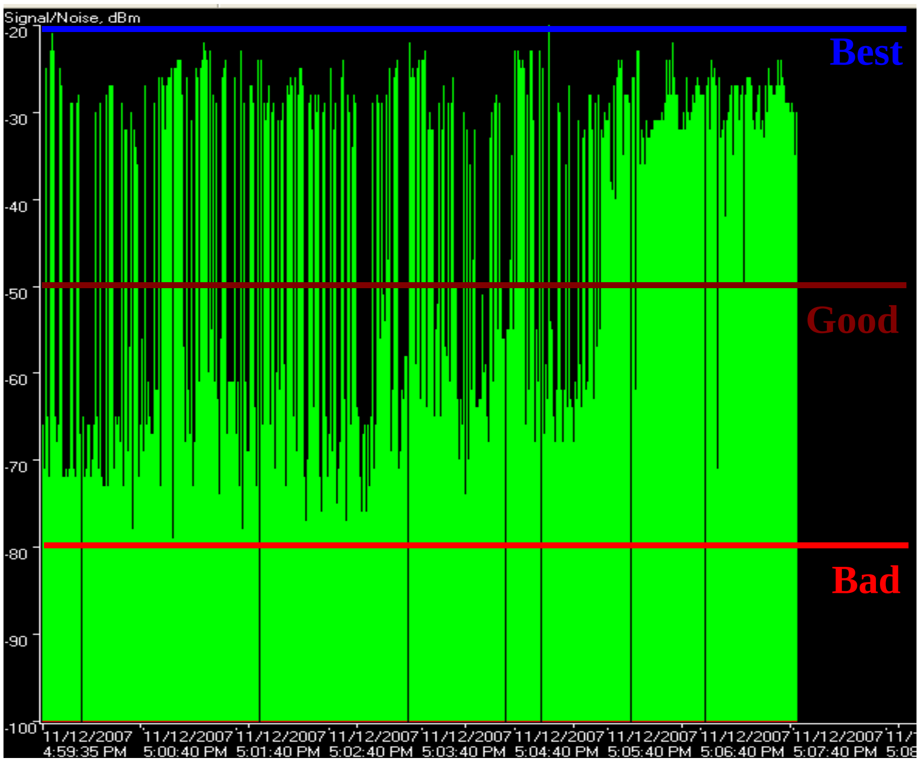


Figure 5-11: SNR Plot of the Wireless Avionics Network in the Presence of 30 Access Points Operating in Channel 11

These tests were performed with a direct line of sight between the CDU and the wireless AHRS unit. The experiment was repeated with the wireless AHRS placed inside a car and the CDU outside the car. As the distance between the two nodes varied with vehicle movement the signal strength also varied accordingly. There was no interference observed from the engine. Figure 5.12 shows the varying signal strength of the wireless link with the rotations of the vehicle.

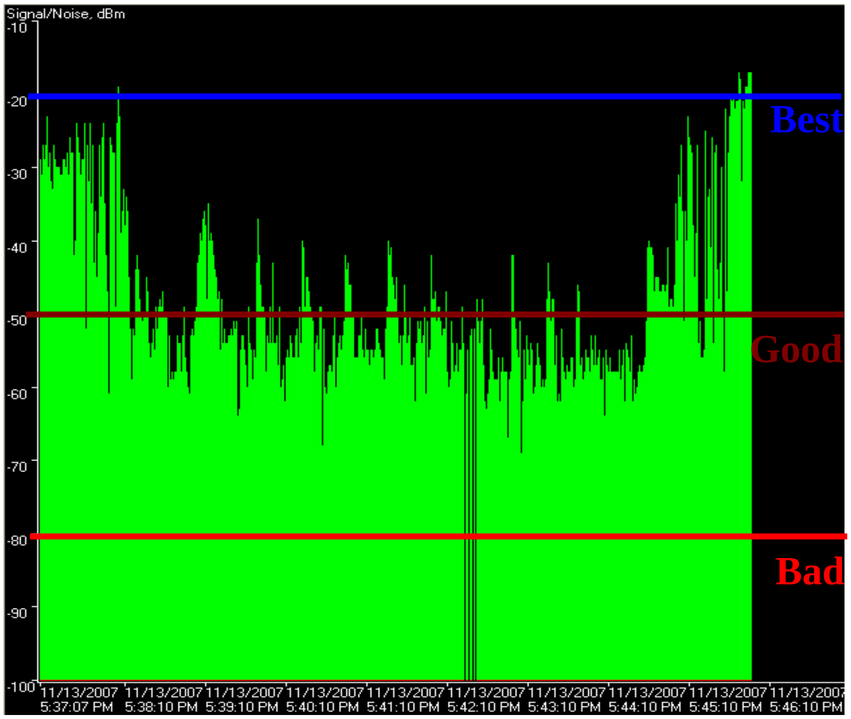


Figure 5-12: SNR Plot of the Wireless Avionics Network in Dynamic Conditions

The experiment was repeated with the two nodes placed inside the Cessna 172 in the hanger. Figure 5.13 shows the CDU placed in the front seat of the C-172. The wireless AHRS was placed in the luggage compartment behind the rear seat. The engine and the electronics were turned off while conducting the performance testing.

Figure 5.14 shows the SNR performance of the wireless link inside the airplane. It can be observed that the signal strength of the wireless link was very high (-15 dBm) compared with the other ground tests mentioned previously.

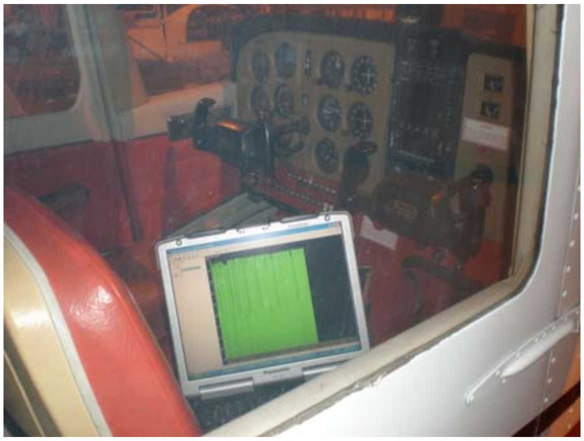


Figure 5-13: CDU Placed inside C-172 for Signal Strength Measurement

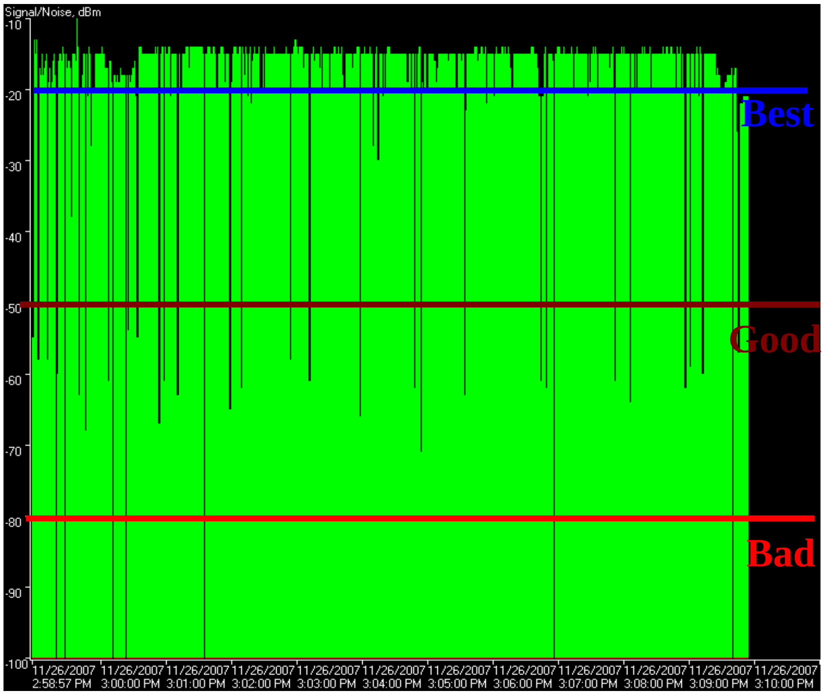


Figure 5-14: SNR Plot of the Wireless Avionics Network inside the C-172

The test drive of the wireless network was conducted in a car with data transmission between the two nodes. The wireless AHRS was strapped to the rear seat of the car and the CDU was placed in the front seat. The drive was conducted for a duration of 992 seconds and the navigational data was logged into a file. The track of the test drive was drawn using MATLAB and is given in Figure 5.15.

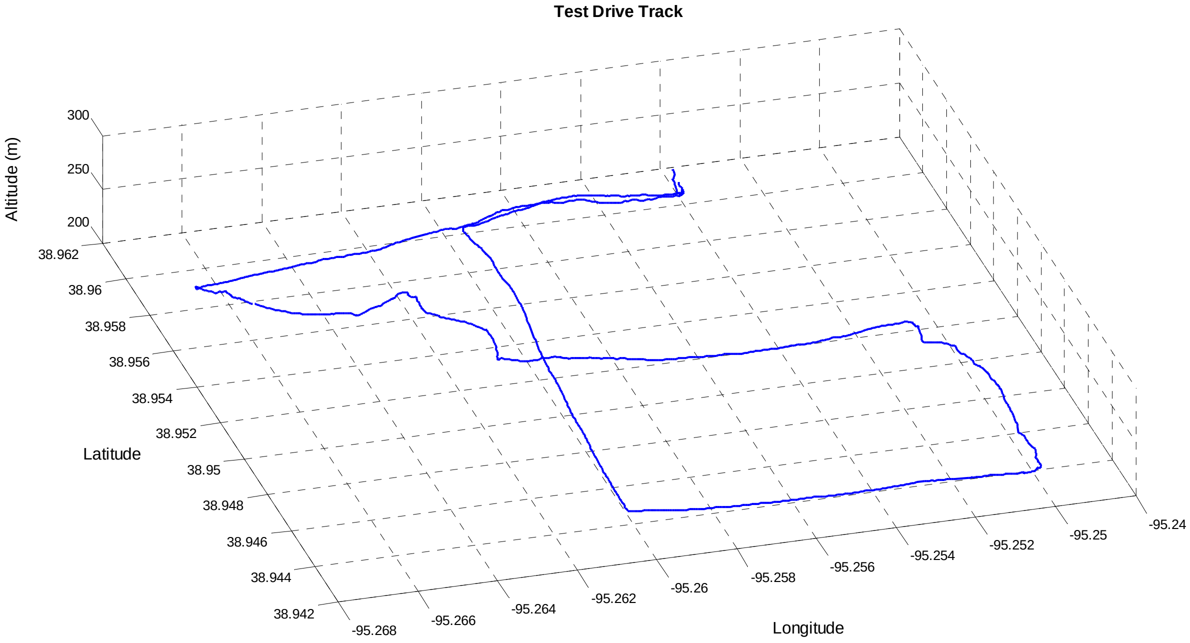


Figure 5-15: Ground Track of the Test Drive

Using *IPSniffer*, the packets transmitted over the wireless network were captured for the performance analysis. Different performance metrics were analyzed using *Ethereal*. Figure 5.16 shows the instantaneous throughput graph obtained from *Ethereal*, with throughput (bytes/sec) shown on the Y-axis and time (seconds) on the X-axis. Figure 5.17 shows the corresponding RTT graph with RTT (milliseconds) on the Y-axis and time (seconds) on the X-axis. No irregularities or discontinuities were found during the entire test.

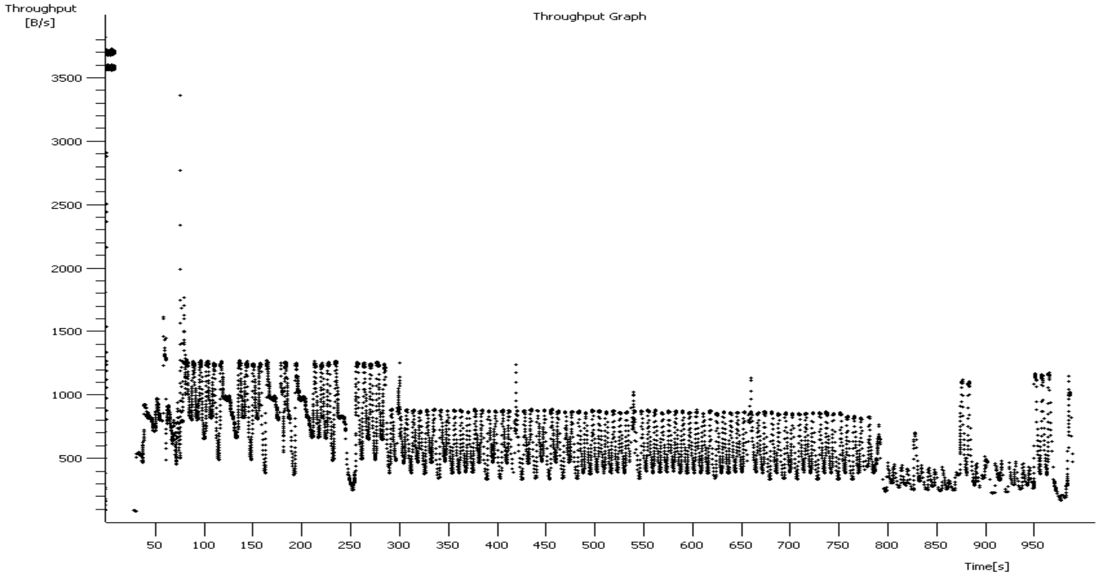


Figure 5-16: Throughput Graph of the Wireless Avionics Network in Test Drive

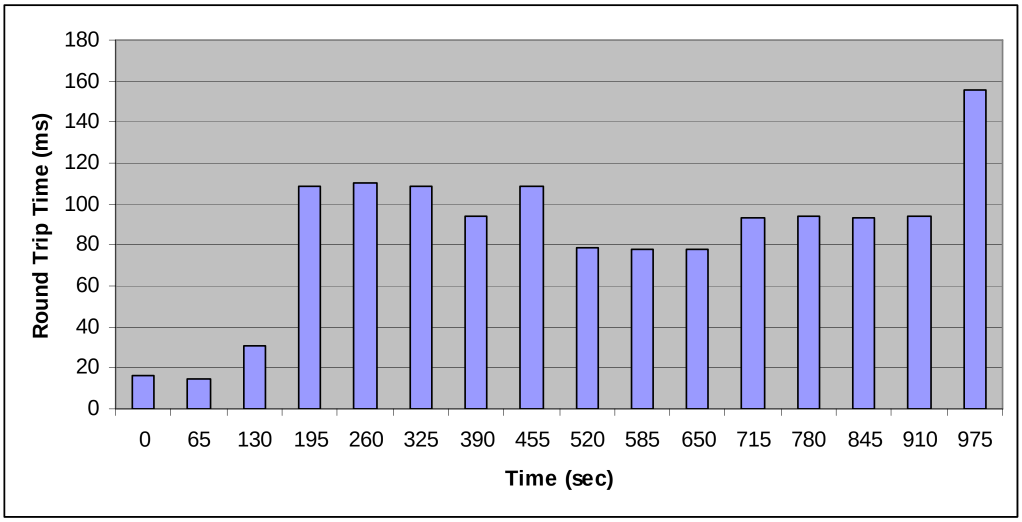


Figure 5-17: Round Trip Time Graph of the Wireless Avionics Network in Test Drive

The duration of the test was 992 seconds, with 8144 packets sent across the network at 8.2 packets/sec. The average packet size was 130 bytes and a total of 1,062,455 bytes were sent at an average speed of 1071.03 bytes/sec (8.4 kbps).

5.3. Flight Test

The results from the ground tests showed the robustness of the IEEE 802.11g based wireless network for ground operations. To determine the performance of the avionics network in actual flight conditions, a flight test was conducted in a Cessna 172. Since the wireless AHRS unit was a self contained box with its own power source, there was no power requirement from the aircraft's power supply. The aircraft was not modified in any way and was thus flown under the standard category. The details of the flight test are given in the flight safety document presented in Appendix A. Figure 5.18 shows the conceptual diagram of the installed wireless avionics network in the C-172.

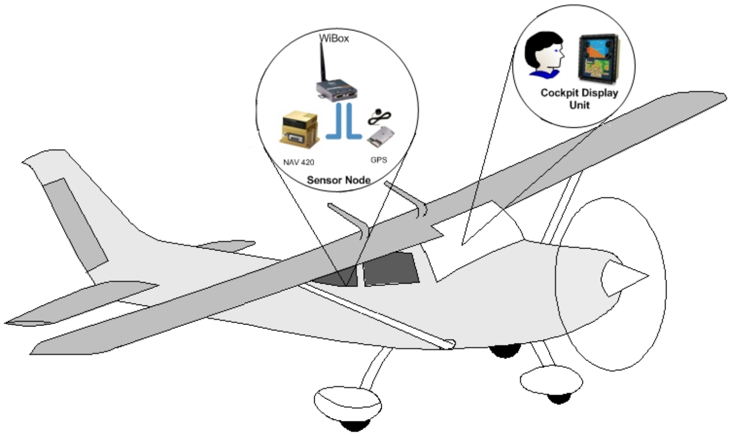


Figure 5-18: Conceptual Diagram of Wireless Avionics Network in C-172

The wireless AHRS was installed into the airplane on the day of the test by creating tie-down points in the enclosure by making holes and using metal wiring. Figure 5.19 shows the wireless AHRS unit installed in the luggage compartment of the C-172. The test set-up was inspected by the pilot before the flight test. The ease of installation of such independent sensor nodes (that have wireless capability and their own source of power) was very evident. There were no modifications required to be done to the airplane for installation.

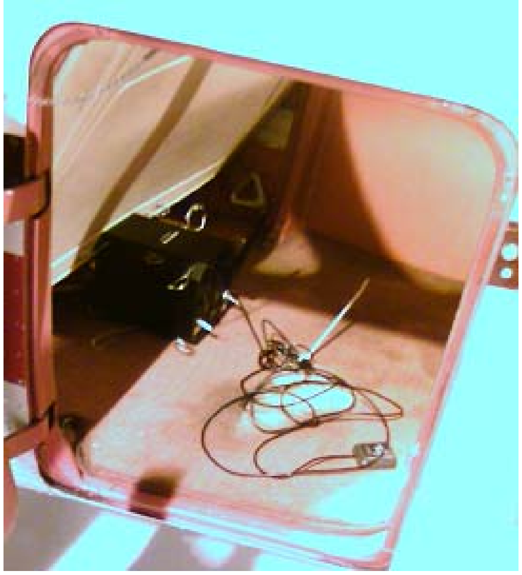


Figure 5-19: Wireless AHRS Unit Installed in the Luggage Compartment of C-172

The flight test was done over a typical flight regime consisting of the following maneuvers: Rate 1 Turns, Steep Turns, Elevator/Rudder/Aileron Short Impulses and Doublets, Sideslip, Slow Flight Turns, Slow Flight, Accelerations and Elevator/Rudder/Aileron Frequency Sweeps. Figure 5.20 describes the timeline of the flight test, with each maneuver located in the order in which it was conducted. The network was also monitored using *IPSniffer* for more than half of the flight.

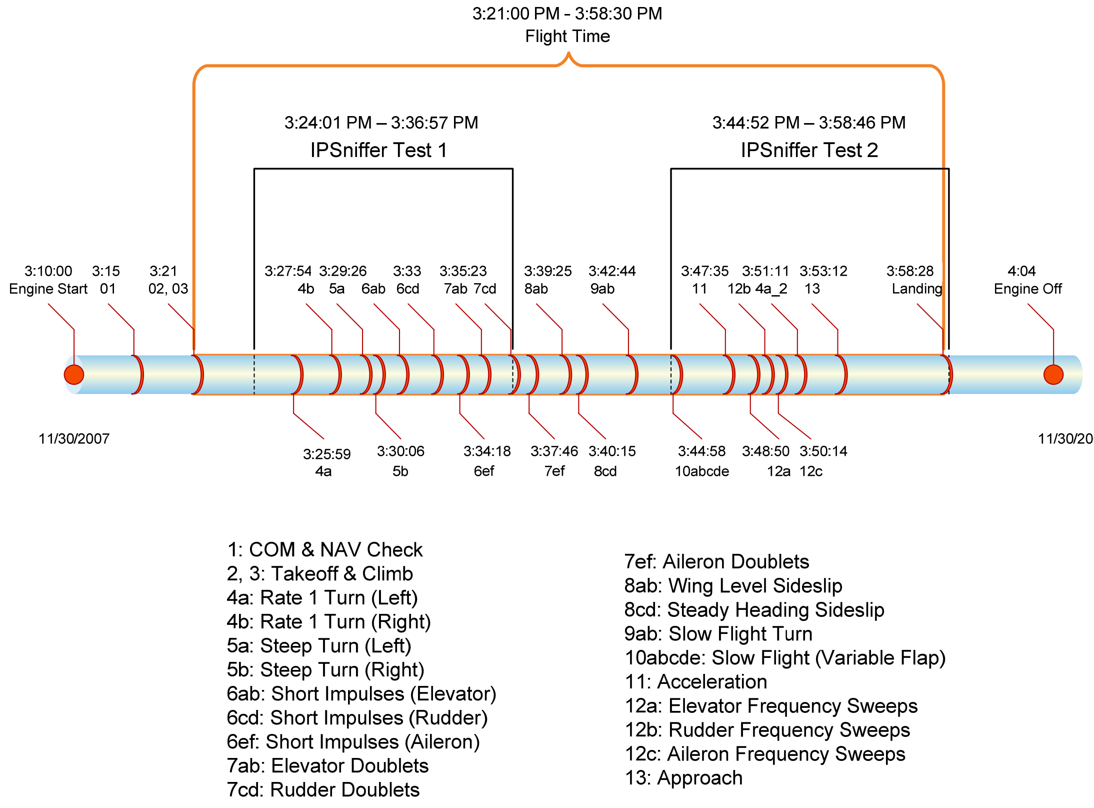


Figure 5-20: Timeline Graph of the Flight Test

The system performance was measured and there were no instances of the network failing. The COMM and NAV checks performed by the pilot before take-off ensured that there was no EMI affecting the functioning of the aircraft's onboard electronic flight instrumentation due to the installed wireless network. The pilot-in-command had no complaints about the wireless test equipment affecting onboard instrumentation at any point during the flight. The flight test procedure consisted of independently logging data from the wireless AHRS for every maneuver from start to stop. Using *IPSniffer*, the packets transmitted in the network were captured for performance analysis.

The results of the data logging from the sensor node are given in Figures 5.21 through 5.28. The transmitted data has been plotted in MATLAB, and the maneuvers are shown in overlay on Google Earth screenshots, with times noting successful data transmittal shown by yellow lines and the missing data by black segments on the trajectory overlays.

From the post-flight data analysis, it was concluded that the network provides a reliable means of data communication in the air. The few discrepancies in data transmission were a result of the cockpit display unit (laptop) trying to connect to other IP addresses. The laptop was installed with several programs like Adobe Acrobat, Microsoft Office Suite, Mozilla Firefox, Internet Explorer et cetera. that look for automatic updates. It is believed that these affected the connectivity of the wireless AHRS to the cockpit display unit. One reason this could have been worse at this location was the presence of community WiFi transmitters providing wireless connectivity at that location. Such significant data losses were observed only during this particular maneuver, the Rate 1 turn to the left. This test was eventually repeated at the end of the flight test, after completion of the rest of the test maneuvers.

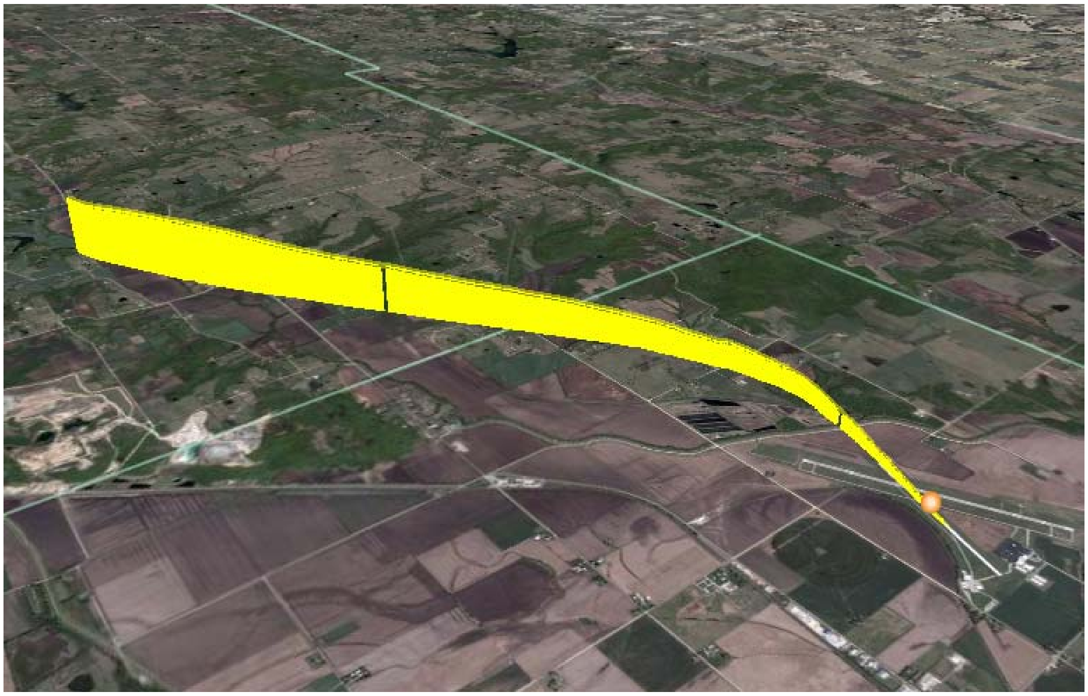


Figure 5-21: Google Earth Screenshot of the Take off and Climb

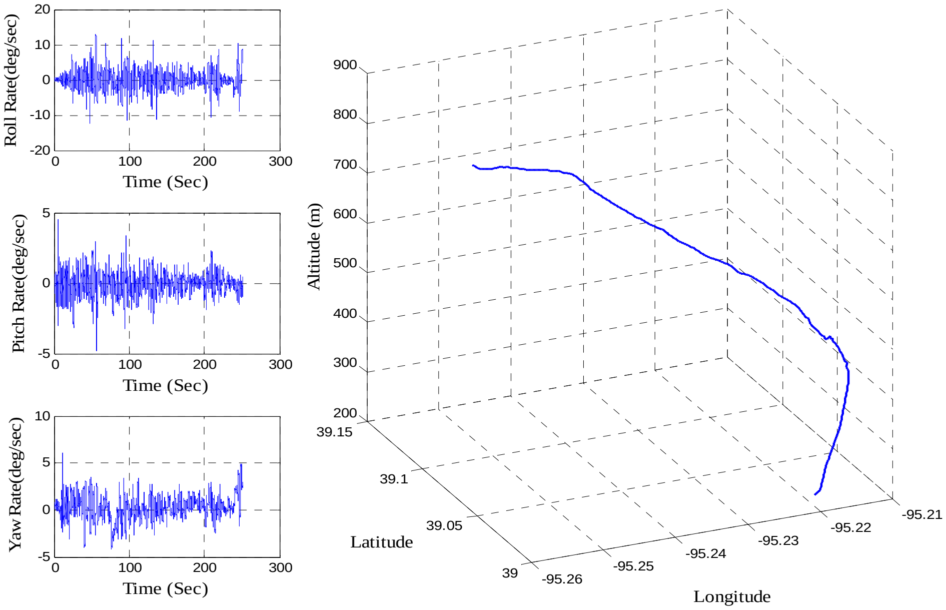


Figure 5-22: Take Off and Climb

The network analysis of the Rate 1 Turn to the left shown in Figures 5.23 and 5.24 was accomplished using *IPSniffer* and is presented in Figure 5.30. This maneuver was subsequently repeated at another physical location to obtain data without the high data loss percentage shown in Figure 5.23 and 5.24. There was considerable data loss due to the laptop trying to connect to other IP addresses. This effect was observed in some ground tests. Solutions to this problem include restricting the essential data communication to channels which are less crowded and also controlling the association of the CDU to other networks.

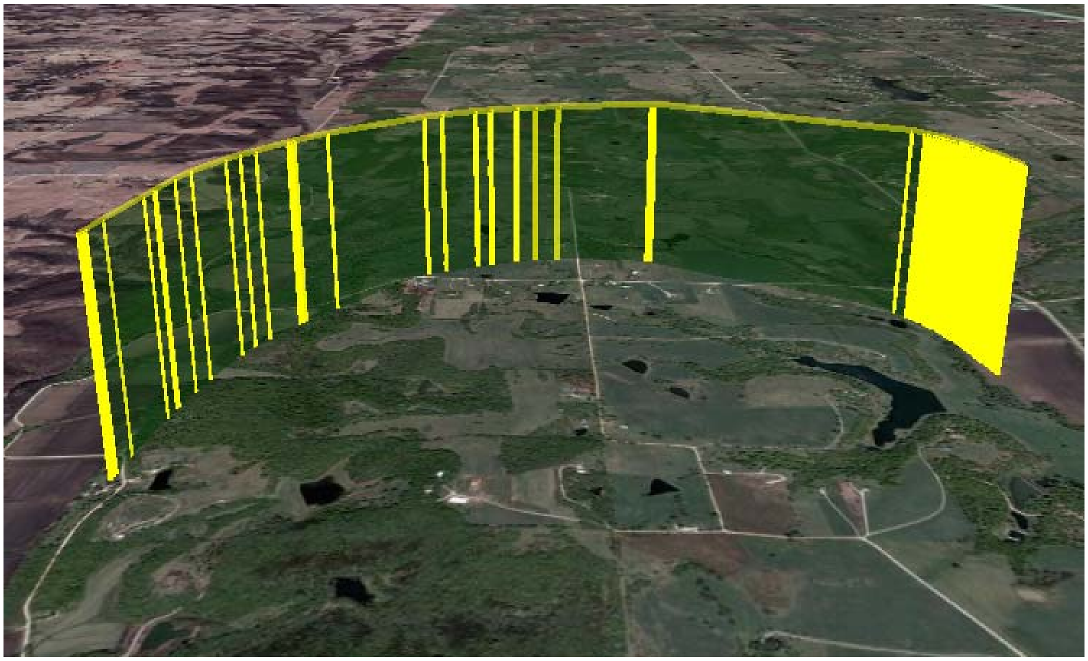


Figure 5-23: Google Earth Screenshot of the First Rate 1 Turn (Left)

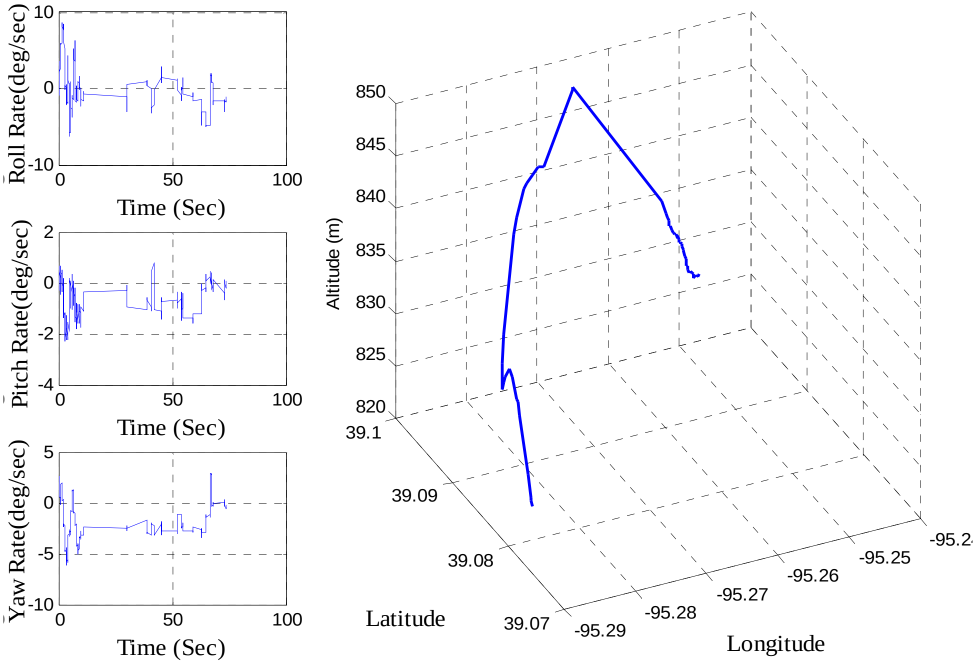


Figure 5-24: First Rate 1 Turn (Left) with Data Losses

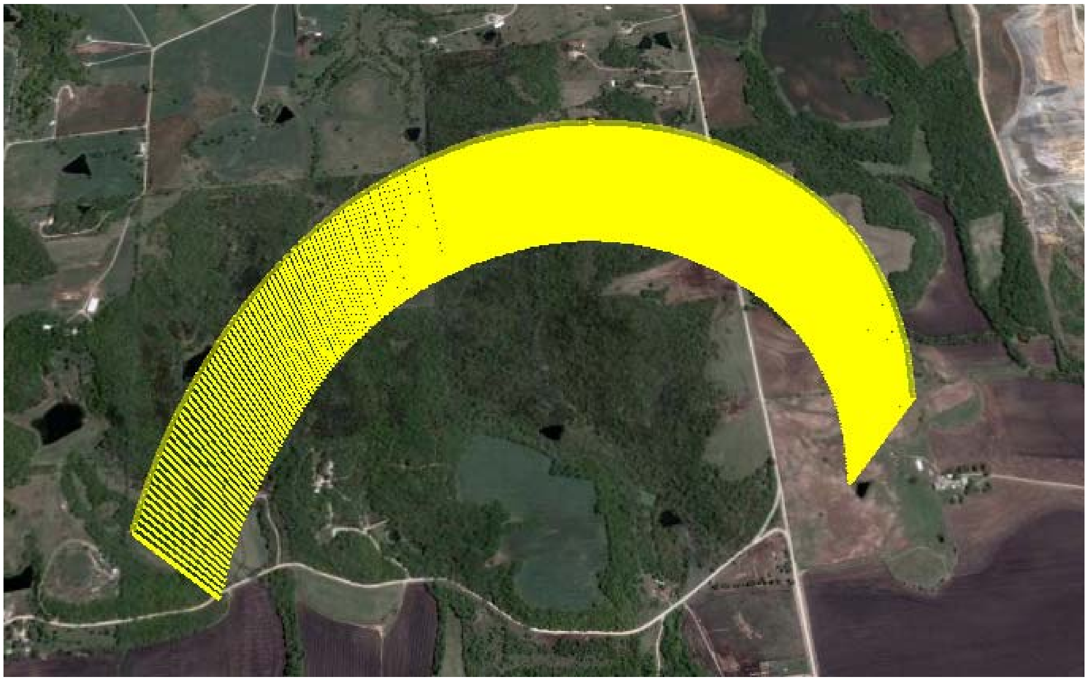


Figure 5-25: Google Earth Screenshot of the Second Rate 1 Turn (Left)

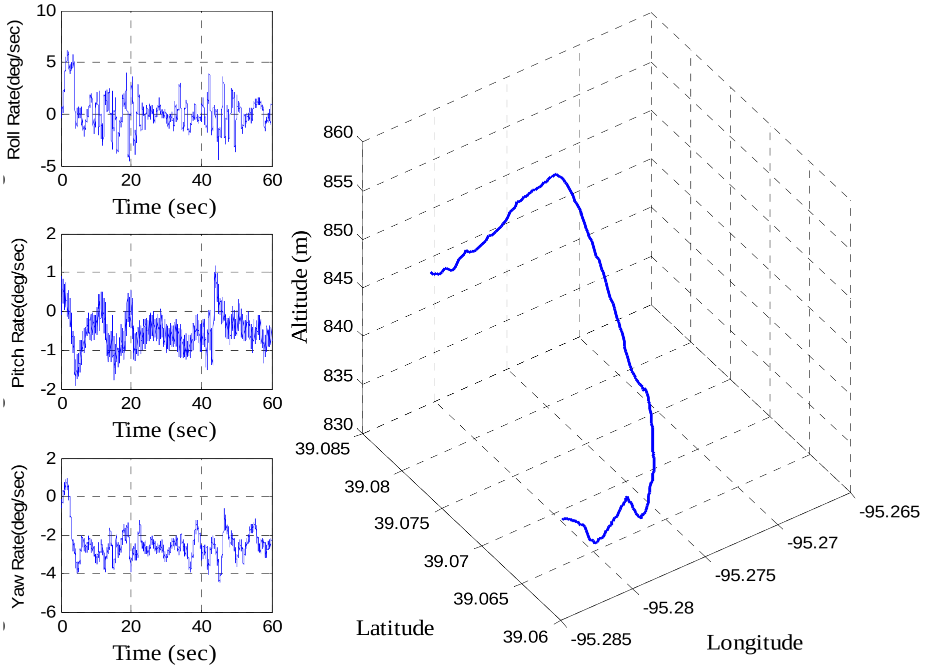


Figure 5-26: Rate 1 Turn (Left)

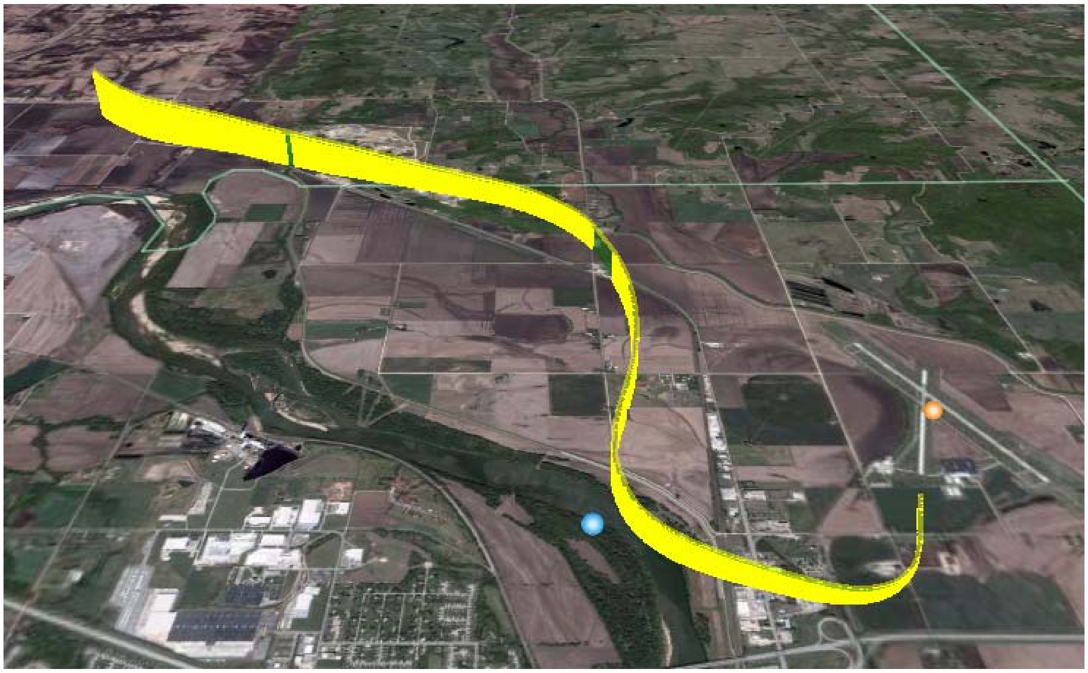


Figure 5-27: Google Earth Screenshot of the Approach and Land

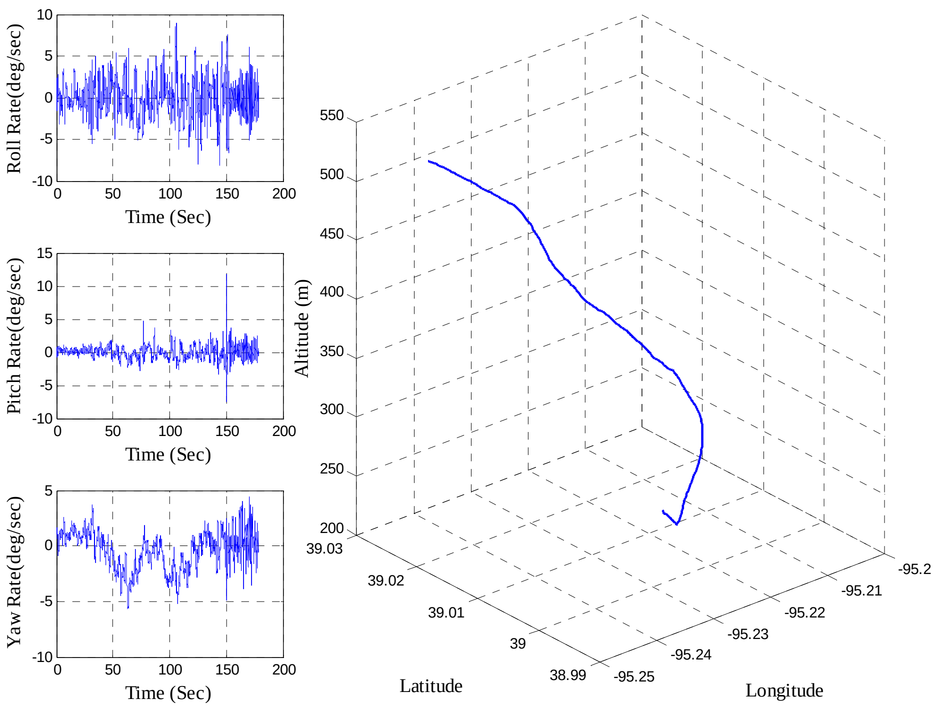


Figure 5-28: Approach and Landing

The test results from *IPSniffer* for the Rate 1 Turn (left) and the other maneuvers are given in Figures 5.30 through 5.36. They were obtained from two capture files. The first captured file was for a duration of 776 sec, with 37,493 packets sent at a rate of 48.3 packets/sec. The average packet size is 112 bytes with a total of 4,203,450 bytes sent across the connection at 5,417 bytes/sec (42 kbps). Figure 5.30 shows the Time Sequence Graph (TSG) for the connection between the wireless AHRS and the CDU. The time sequence is a graph of the TCP sequence number versus time. This would be a constantly increasing straight line for a normal connection where there are no inconsistencies due to segment losses, duplicate ACK, retransmissions, etc. The letter *R* in TSG represents areas where retransmissions have occurred. It was observed that there were lost segments and duplicate acknowledgments in the initial few seconds, which affected the throughput at the beginning of testing. This was followed by multiple TCP connections from the CDU to different IP addresses. This can be observed from 140 seconds to nearly 180 seconds from the start of the test. Multiple retransmissions were observed in the enlarged section. Because of the multiple SYN packets sent by the CDU, the network had high data losses which can be observed during the Rate 1 Turn to left in Figure 5.23. The throughput and RTT of the network are given in Figures 5.31 and 5.32 respectively. The blue line in the throughput graph gives the average throughput of the connection to that point. The throughout decreased during the data losses and retransmissions seen during the Rate 1 Turn. Different TCP connections during this period are shown in Figure 5.33.

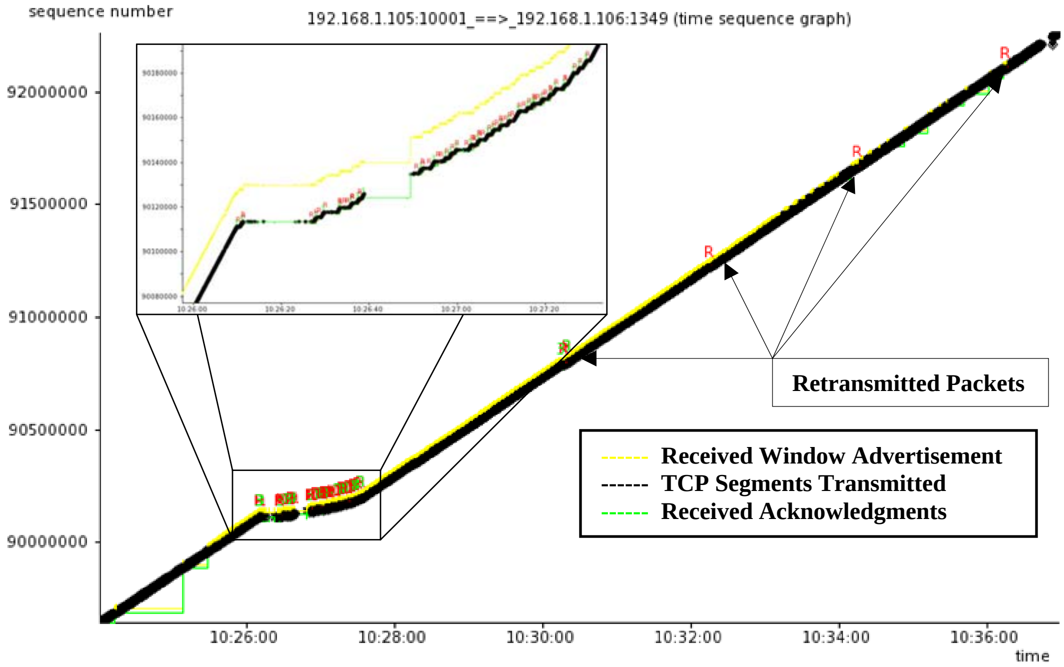


Figure 5-29: Time Sequence Graph from IPSniffer Test 1

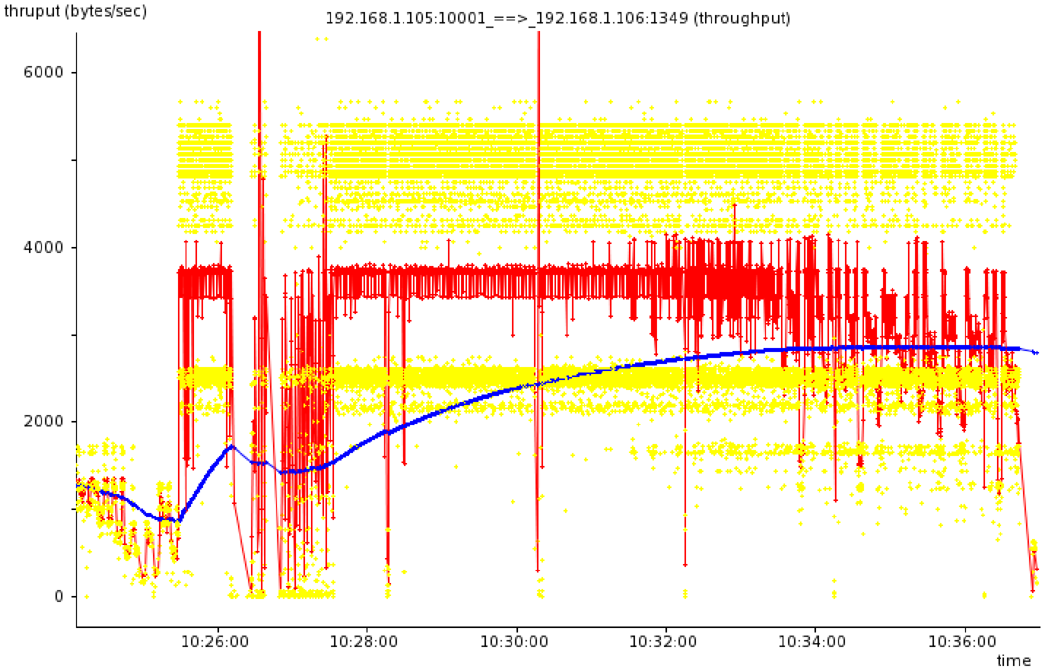


Figure 5-30: Throughput Graph from IPSniffer Test 1

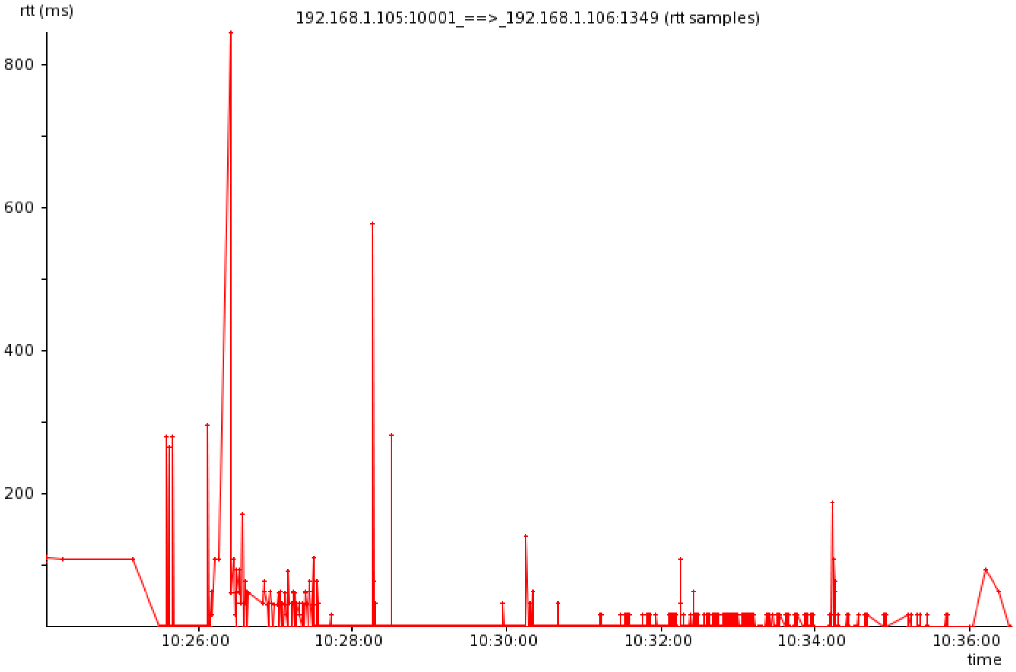
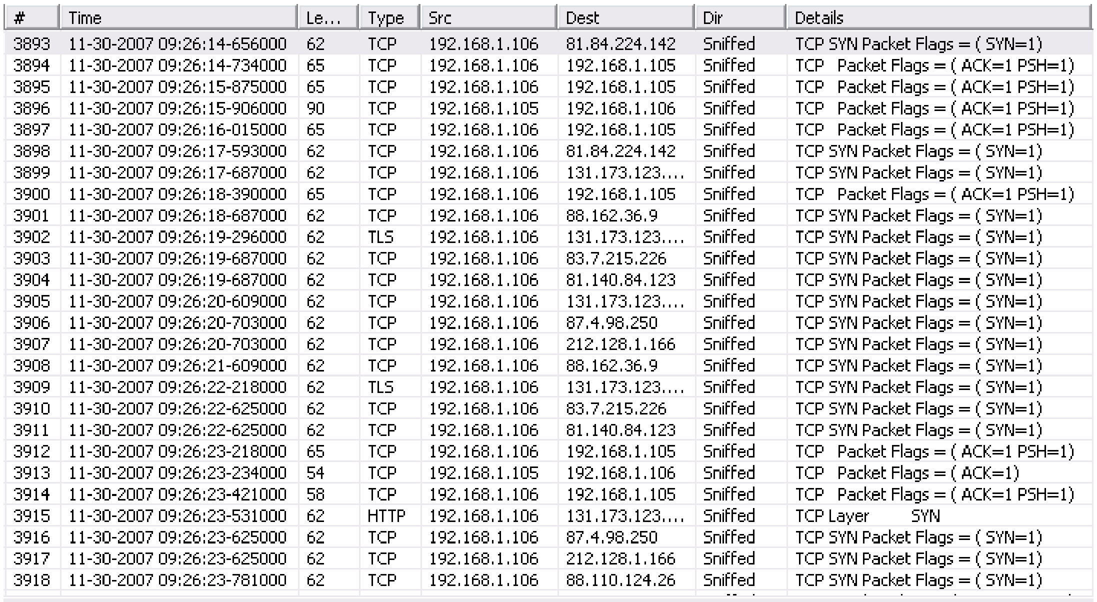


Figure 5-31: RTT Graph from IPSniffer Test 1



#	Time	Le...	Type	Src	Dest	Dir	Details
3893	11-30-2007 09:26:14-656000	62	TCP	192.168.1.106	81.84.224.142	Sniffed	TCP SYN Packet Flags = (SYN=1)
3894	11-30-2007 09:26:14-734000	65	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3895	11-30-2007 09:26:15-875000	65	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3896	11-30-2007 09:26:15-906000	90	TCP	192.168.1.105	192.168.1.106	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3897	11-30-2007 09:26:16-015000	65	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3898	11-30-2007 09:26:17-593000	62	TCP	192.168.1.106	81.84.224.142	Sniffed	TCP SYN Packet Flags = (SYN=1)
3899	11-30-2007 09:26:17-687000	62	TCP	192.168.1.106	131.173.123....	Sniffed	TCP SYN Packet Flags = (SYN=1)
3900	11-30-2007 09:26:18-390000	65	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3901	11-30-2007 09:26:18-687000	62	TCP	192.168.1.106	88.162.36.9	Sniffed	TCP SYN Packet Flags = (SYN=1)
3902	11-30-2007 09:26:19-296000	62	TLS	192.168.1.106	131.173.123....	Sniffed	TCP SYN Packet Flags = (SYN=1)
3903	11-30-2007 09:26:19-687000	62	TCP	192.168.1.106	83.7.215.226	Sniffed	TCP SYN Packet Flags = (SYN=1)
3904	11-30-2007 09:26:19-687000	62	TCP	192.168.1.106	81.140.84.123	Sniffed	TCP SYN Packet Flags = (SYN=1)
3905	11-30-2007 09:26:20-609000	62	TCP	192.168.1.106	131.173.123....	Sniffed	TCP SYN Packet Flags = (SYN=1)
3906	11-30-2007 09:26:20-703000	62	TCP	192.168.1.106	87.4.98.250	Sniffed	TCP SYN Packet Flags = (SYN=1)
3907	11-30-2007 09:26:20-703000	62	TCP	192.168.1.106	212.128.1.166	Sniffed	TCP SYN Packet Flags = (SYN=1)
3908	11-30-2007 09:26:21-609000	62	TCP	192.168.1.106	88.162.36.9	Sniffed	TCP SYN Packet Flags = (SYN=1)
3909	11-30-2007 09:26:22-218000	62	TLS	192.168.1.106	131.173.123....	Sniffed	TCP SYN Packet Flags = (SYN=1)
3910	11-30-2007 09:26:22-625000	62	TCP	192.168.1.106	83.7.215.226	Sniffed	TCP SYN Packet Flags = (SYN=1)
3911	11-30-2007 09:26:22-625000	62	TCP	192.168.1.106	81.140.84.123	Sniffed	TCP SYN Packet Flags = (SYN=1)
3912	11-30-2007 09:26:23-218000	65	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3913	11-30-2007 09:26:23-234000	54	TCP	192.168.1.105	192.168.1.106	Sniffed	TCP Packet Flags = (ACK=1)
3914	11-30-2007 09:26:23-421000	58	TCP	192.168.1.106	192.168.1.105	Sniffed	TCP Packet Flags = (ACK=1 PSH=1)
3915	11-30-2007 09:26:23-531000	62	HTTP	192.168.1.106	131.173.123....	Sniffed	TCP Layer SYN
3916	11-30-2007 09:26:23-625000	62	TCP	192.168.1.106	87.4.98.250	Sniffed	TCP SYN Packet Flags = (SYN=1)
3917	11-30-2007 09:26:23-625000	62	TCP	192.168.1.106	212.128.1.166	Sniffed	TCP SYN Packet Flags = (SYN=1)
3918	11-30-2007 09:26:23-781000	62	TCP	192.168.1.106	88.110.124.26	Sniffed	TCP SYN Packet Flags = (SYN=1)

Figure 5-32: Multiple Connections from CDU in IPSniffer Test 1

The second capture file was for a duration of 835 sec, with 40,349 packets sent at a rate of 48.35 packets/sec. The average packet size is 112 bytes, with a total of 4,552,027 bytes sent across the connection at 5,455 bytes/sec (43 kbps). Figure 5.34 shows the Time Sequence Graph of the TCP stream during the second test. Though there were less TCP SYN packets sent from the CDU, a few packet losses were observed at 470 seconds and at 640 seconds. The retransmissions of the lost segments can be observed from the thin lines shown at the top right corner of the graph. This affected the throughput and resulted in higher round trip times. The network connection was better than that during the first test. The wireless connection performed reliably, with no data losses in any of the maneuvers conducted during this period. The throughput and RTT of the network are given in Figures 5.35 and 5.36 respectively.

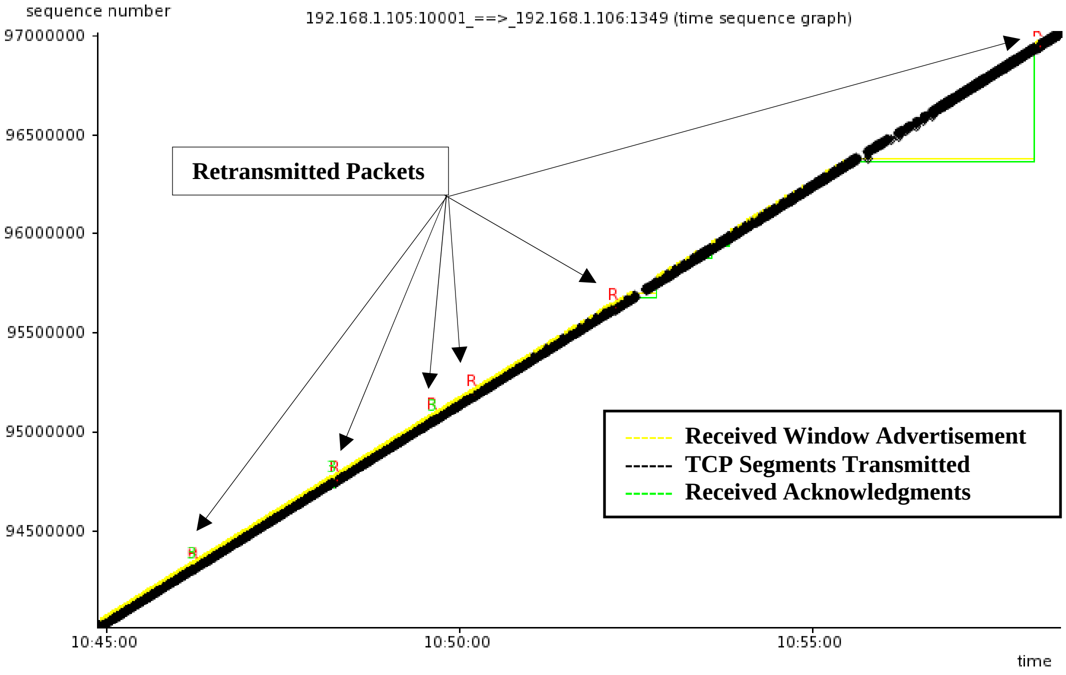


Figure 5-33: Time Sequence Graph from IPSniffer Test 2

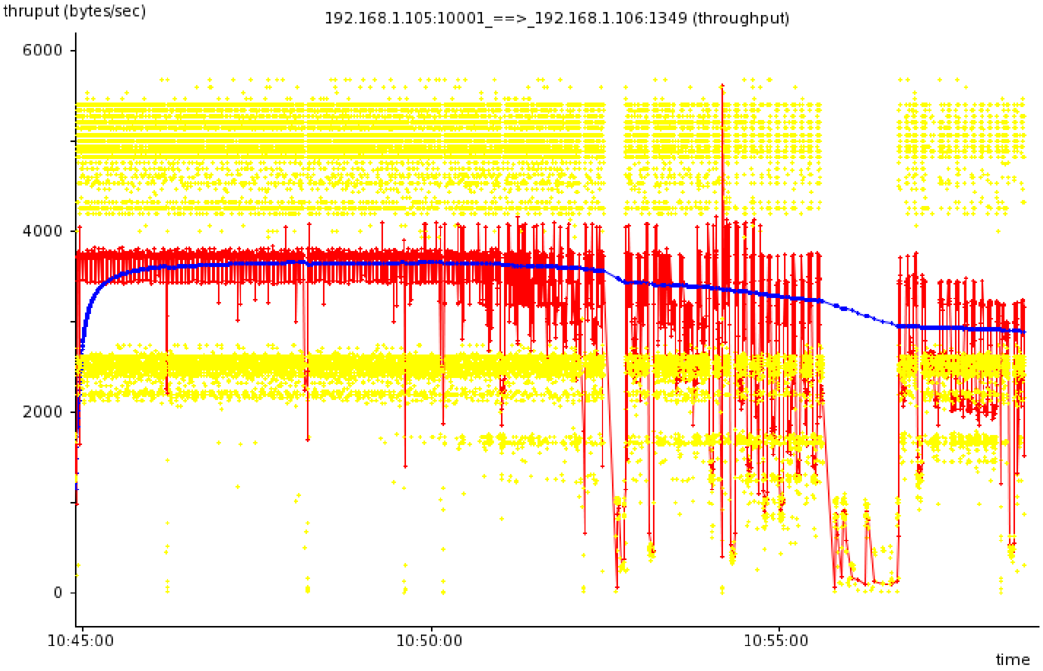


Figure 5-34: Throughput Graph from IPSniffer Test 2

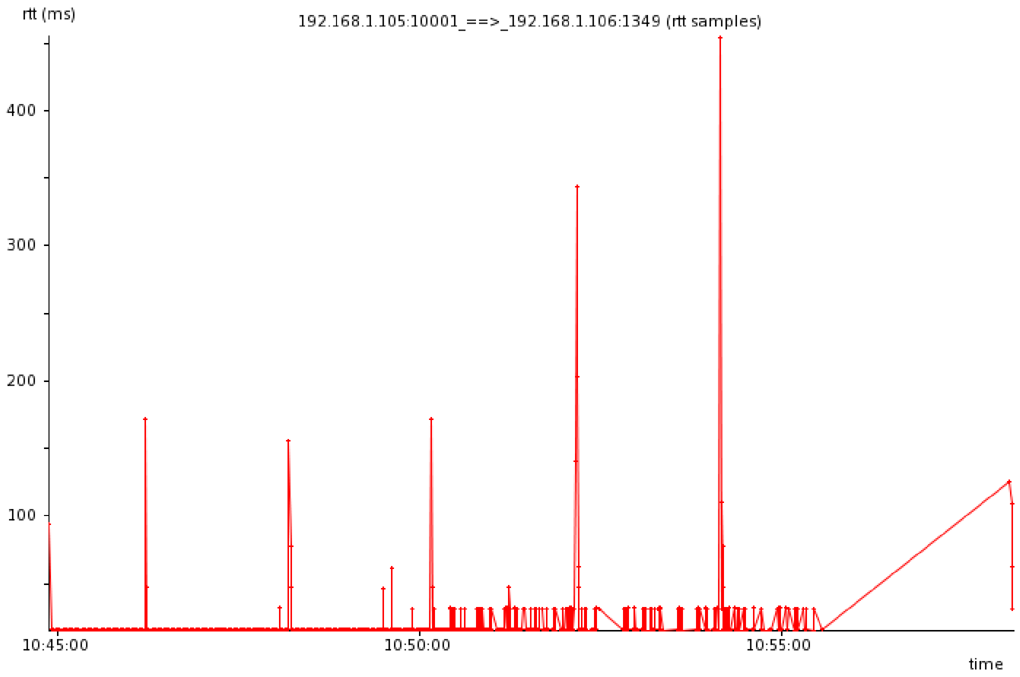


Figure 5-35: RTT Graph from IPSniffer Test 2

Congestion in the network can be analyzed using retransmissions and duplicate acknowledgements (Dup ACKs). Whenever there is a packet loss or acknowledgement loss, the sender retransmits the packets again. Loss of service was measured approximately by analyzing the retransmissions, duplicate acknowledgements and network idle times. Since the capturing of the packets was done at the receiver end, there is no direct way to measure the absolute packet loss in the network.

From the IPSniffer Test 1, there were 89 retransmission packets and 518 Dup ACKs that were accounted as lost due to congestion (1.525%). It was observed that there were no packets captured for 45 seconds. This was accounted for as a loss of the connection (5.79%). The unwanted connections observed from multiple SYN packets constituted approximately 1.62% of the total connection time. Table 5.2 shows the summary of the network statistics. Figure 5.36 gives the overall percentage statistics of the connection.

Total Time	776 sec	**Actual Transmission Time**	731 sec
Successful Connection	706.5508 sec	**Total Packets Sent**	37,493
Loss due to Congestion	11.83466 sec	**Retransmissions**	89
Loss due to SYN Packets	12.61454 sec	**Duplicate ACKs**	518
Loss of Connection	45 sec	**SYN Packets**	647
		Successful Packets	36,239

Table 5-2: Performance Statistics of IPSniffer Test 1

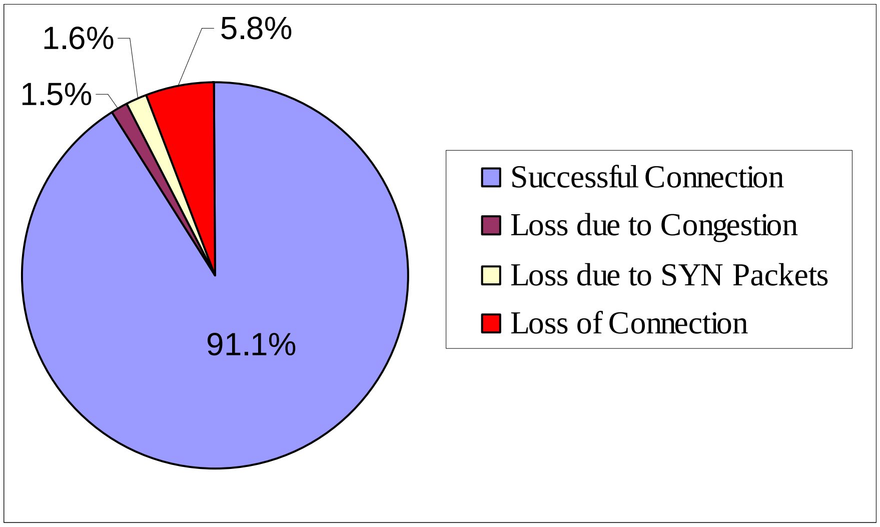


Figure 5-36: Performance Summary of IPSniffer Test 1

From the IPSniffer Test 2, there were only 18 retransmission packets and 37 Dup ACKs that were accounted for as losses due to congestion (0.12%). No packets were transmitted for 62 seconds. This was accounted for as due to the loss of the connection (7.4%). The unwanted connections observed from multiple SYN packets constituted approximately 1.44% of the total connection time. Table 5.3 shows the summary of the network statistics. Figure 5.37 gives the overall percentage statistics of the connection.

Total Time	835 sec	**Actual Transmission Time**	773 sec
Successful Connection	759.2638 sec	**Total Packets Sent**	40349
Loss due to Congestion	0.996431 sec	**Retransmissions**	18
Loss due to SYN Packets	11.99341 sec	**Duplicate ACKs**	37
Loss of Connection	62 sec	**SYN Packets**	662
		Successful Packets	39632

Table 5-3: Performance Statistics for IPSniffer Test 2

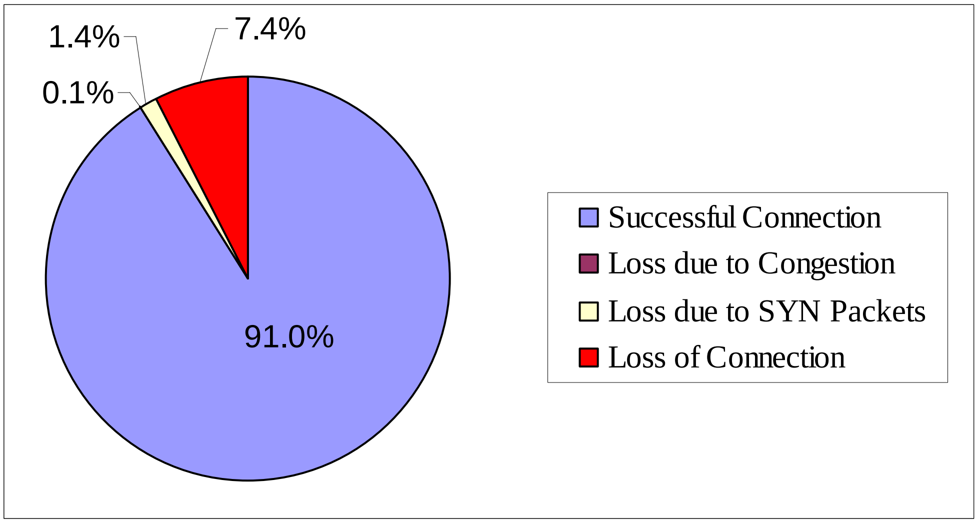


Figure 5-37: Performance Summary of IPSniffer Test 2

As mentioned earlier, the data from the wireless AHRS was recorded for each maneuver separately for post processing. In general, these flight maneuvers are conducted to derive the flight dynamics from the aircraft's attitude data. Table 5-4 shows the sensor activity during the flight maneuvers. Log time is the total time it took to complete each maneuver. During this time the sensor data is being logged. The AHRS unit was set to transmit NAV packets consisting of pitch, roll, and yaw angles, longitude, latitude, altitude, GPS velocity, and the angular rates. The maximum rate at which the NAV420 can transmit the data is 100 Hz. The number of NAV packets recorded and the average output rate of the sensor is shown in Table 5-4. Figure 5-38 is the histogram of Table 5-4.

Flight Maneuver	Log Time (sec)	Packets Recorded	Sensor Update Rate (Hz)
Take off	281	27503	97.88
Rate 1 Turn (Left)	74	1278	17.39
Rate 1 Turn (Left) Repeat	57	5703	99.70
Rate 1 Turn (Right)	58	5518	95.77
Steep Turn (Left)	30	2372	79.07
Steep Turn (Right)	27	2308	84.85
Short Impulses Elevator	40	3590	89.75
Short Impulses Rudder	30	2803	93.43
Short Impulses Aileron	14	1241	88.64
Elevator Doublets	27	2676	99.11
Rudder Doublets	25	2408	96.32
Aileron Doublets	27	2456	90.96
Winglevel Sideslip	31	2970	95.81
Steady Heading Sideslip	45	4388	97.51
Slow Flight Turn	67	6225	92.91
Slow Flight with Varying Flap	134	12260	91.49
Accelerated Flight	25	2383	95.32
Elevator Frequency Sweeps	24	2372	98.83
Rudder Frequency Sweeps	23	2220	96.52
Aileron Frequency Sweeps	21	2091	99.57
Approach and Landing	178	17138	96.28

Table 5-4: Sensor Update Rate for Different Maneuvers

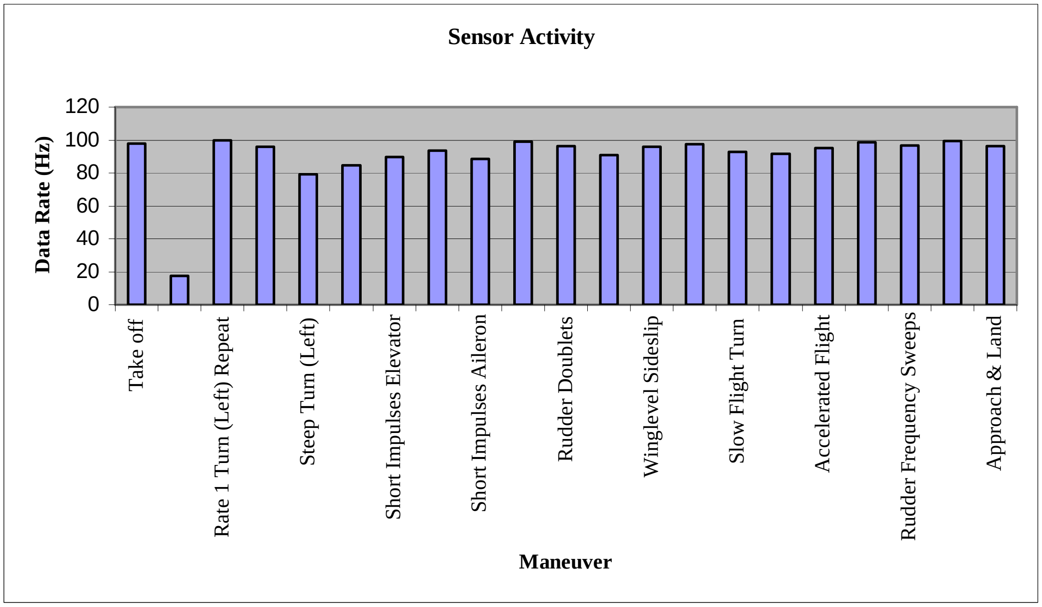


Figure 5-38: Sensor Update Rate

It can be observed that the average update rate is 17 Hz during the Rate 1 turn to the left. On average, the update rate of the sensor during flight test is 91 Hz. Most of the AHRS units, which are used in commercial airplanes, have an update rate of 60 – 100 Hz. The acceptable rate is 25 – 50 Hz, depending on the controller design. Good wireless network performance was demonstrated during all maneuvers with an exception during the Rate 1 turn.

A plot from the *IPSniffer* tool showing protocol activity is given in Figure 5.39. The wireless connection is dominated by the TCP protocol throughout the test. The UDP connection protocol being used results from the computer sending out initial contact messages to other detected IP addresses. Reducing this activity will improve system performance as previously noted. From the captured files it is found that 98.3% of the total TCP packets transmitted are the data packets between the CDU and wireless AHRS.

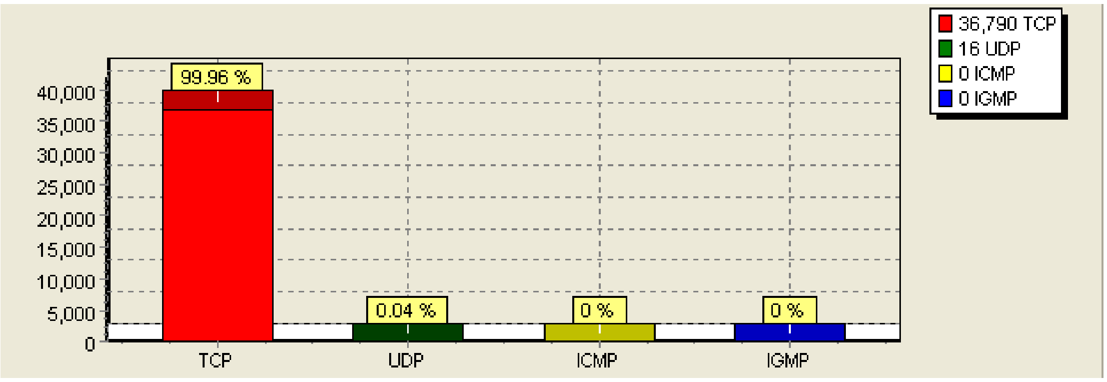


Figure 5-39: Protocol Activity from the IPSniffer Tool

The signal strength of the connection, tested immediately after landing and during taxing with the engine still running, is shown in Figure 5.40. A consistent signal strength of approximately -20 dBm reflects good network performance.

The results from the flight test demonstrate the usability and reliability of the WiFi based network. The network is very easily installed for testing. Similarly, it can easily be uninstalled after testing. It did not require any modification to the aircraft, and does not interfere with the onboard instrumentation. This is a major consideration favoring the use of WiFi based independent sensor nodes for flight testing. The signal strength and the throughput analysis of the network reflect the robust characteristics of the WiFi based network for flight instrumentation. Instances of the network being affected by other IP addresses, decreasing the availability of the computer, need to be studied and analyzed in detail to avoid data losses and reductions in throughput.

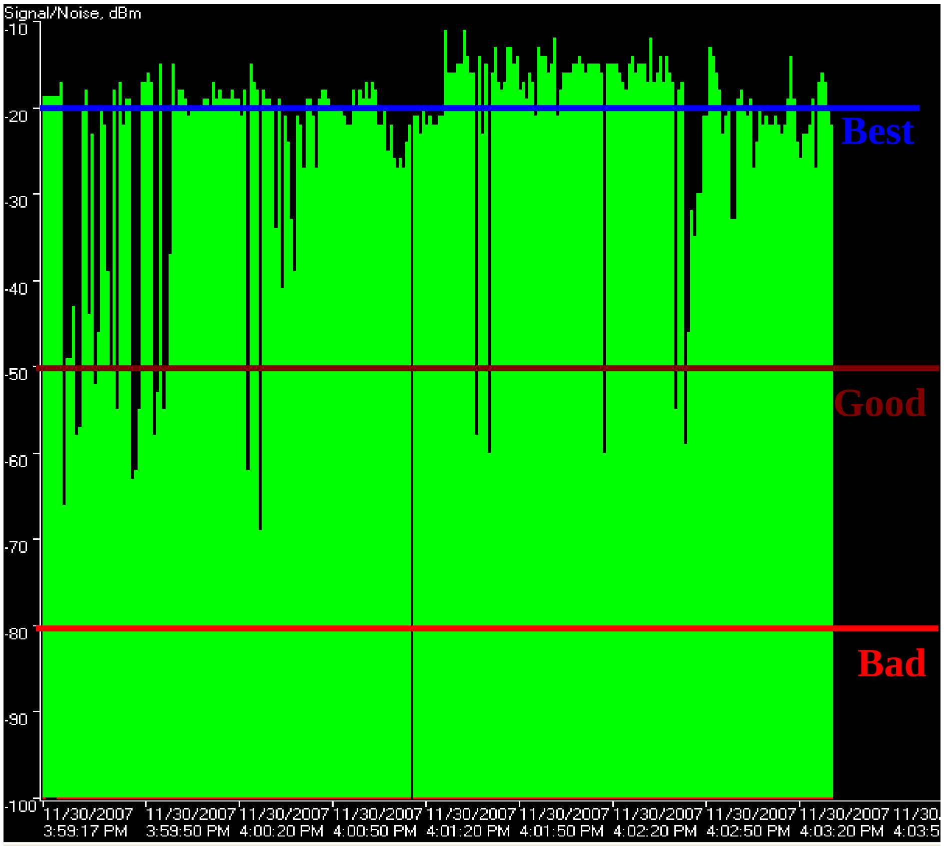


Figure 5-40: SNR Performance Graph during Taxing

6. Summary and Conclusions

6.1. Summary

This work has focused on the development and testing of IEEE 802.11a/b/g standards for their applications in aviation. Various open source tools were studied to analyze and troubleshoot the network. The wireless link performed reliably during various operating conditions on the ground and during the flight test. Another favoring condition is that there was no interference observed from the wireless equipment to the onboard avionics during the flight test. The degradation in the network performance observed during the flight due to the multiple SYN packets from the CDU can be controlled. It is interesting to find that the performance of the wireless avionics network was far better than on the ground (43 Kbps in flight and 8.4 Kbps on the ground). It is very easy to install wireless based instrumentation for flight testing. Apart from the high data rates and security offered by WiFi protocols, they also offer flexibility in installation and maintenance. Unlike proprietary aviation data communication standards these commercial standards are very inexpensive to implement. WiFi will save on the costs involved in the miles of copper wiring, in the airframe modifications, and in the man-hours required for installations. They can be feasible alternatives to implement for flight testing. Various wireless security standards have been discussed. These provide a good reference for understanding the security capabilities of the COTS products.

6.2. Conclusions

As wireless technology matures, its adaptability to the general aviation field is very likely. The results from the performance analysis tests, both on the ground and in flight, are very promising. WLAN standards support high data rates which are sufficient for most general aviation avionics and flight testing applications. Use of COTS hardware and software greatly reduces the development costs of the avionics network. Significant research is needed to determine the suitability of this wireless standard for mission-critical applications in which a higher level of reliability is demanded. This work is a successful starting point for the fly-by-wireless concept.

7. Future Work

It would be appropriate to test the WiFi protocols for data intense applications, such as real time video transmission for cabin and airplane monitoring. During the flight test there was no direct line of sight between the two wireless nodes. At the same time there were no metal obstacles between them. In an actual flight application the output could change considerably with the location of the wireless instruments. It is necessary to compare the performance of the wireless network under different flight scenarios. For a better analysis of the network, it is necessary to capture the trace from both the sender and the receiver. Free space path losses, and path losses within the airplane, need to be studied. This will help in the estimation of possible signal losses when the wireless nodes are placed at various locations within the airplane. Higher data rates depend on the signal strength and the receiver sensitivity. The use of high gain antennas and amplifiers should be considered, based on the application, to improve the signal strength. Though there was no interference observed during the flight test, it is important to determine the radio environment present in the airplane using spectrum analyzers. Most critical data applications demand that the communications be deterministic, in the sense that each sensor will have guaranteed time slots for communication. Apart from throughput and RTT, Quality of Service (QoS) is a performance metric relating the loss of service, latency, jitter, et cetera. These should be considered for future work. The acceptable data loss depends on the update rate and latency requirements, which in turn depend on the system design. Different systems will have different performance requirements and thus different acceptable losses and update rates. The performance of the wireless network should be compared against the maximum data losses allowed by that system. It will be crucial to evaluate the WiFi protocols for such applications. Though an overview of the security standards has been given, they have not been analyzed for their performance. A rigorous analysis of these algorithms should be considered as a component of the future work.

The performance of the WiFi system has to be measured when multiple networks are in operation simultaneously within the airplane. The results should be compared when multiple networks are using the same channel and when different channels are used. New standards, such as IEEE 802.11n and IEEE 802.16, which offer improved performance metrics, also need to be compared for their suitability against WiFi for avionics applications. It is also important to consider heterogeneous applications onboard an aircraft, where multiple wireless standards based on applications will be operating together without being effected by each other. Network security is of primary importance in the development of the wireless avionics network. Metrics required to characterize various security standards for avionics applications have to be studied.

8. References

1) J. Ned Yelverton: *Wireless Avionics*, IEEE Digital Avionics Systems Conference, 1995, 14th DASC, 5-9 Nov 1995 pages 95-99.
2) Michael Gandy, Lockheed Martin: *Wireless Sensors for Aging Aircraft Health Monitoring*. URL: http://www.jcaa.us/AA_Conference_2001/Papers/7B_2.pdf.
3) Dryden Flight Research Center: "Radio-Frequency Wireless Flight-Control System".
   URL: http://www.dfrc.nasa.gov/Newsroom/X-Press/1999/Mar26/news.html.
4) http://www.invocon.com/WFCS_tech_overview.html.
5) http://www.ueet.nasa.gov/toi/viewtoi.php?id=98.
6) http://www.honeywell.com/sites/aero/Communication_Navigation_Systems3_C2BB6B07D-BE5D-1863-8A9A-D7F4A616C4EC_H3286B641-92EB-BB9B-8960-148D029122C0.htm.
7) White Paper – Securaplane Technologies Inc.: *SecuraNet™ WIRELESS TECHNOLOGY Intra-Aircraft Wireless Data Bus for Essential and Critical Applications*.
8) Tom Karygiannis, Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", Special Publication 800-48, National Institute of Standards and Technology.
9) "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).
10) "IEEE 802.11b Wireless LANs", 3Com Corporation.
    URL: http://www.3com.com/other/pdfs/infra/corpinfo/en_US/50307201.pdf
11) "Introduction to IEEE 802.11".
    URL: http://www.intelligraphics.com/articles/80211_article.html
12) Mark Prowten, "Encryption Technology for Embedded Network Devices", Industrial Ethernet Book Issue 26:31.
    URL: http://wireless.industrial-networking.com/articles/articledisplay.asp?id=514

13) "Encryption and Its Importance to Device Networking", Lantronix Inc.

14) Stanley Wong, "The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards", SANS Institute 2003.

15) Windows Platform Design Notes: "WiFi Protected Access (WPA) Overview".

16) Wi-Fi Alliance: "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks", April 29, 2003.

17) Jim Geier, "802.11 Security Beyond WEP", June 26, 2002.
URL: http://www.wi-fiplanet.com/tutorials/article.php/1377171

18) Jim Geier, "WPA Security Enhancements", March 20, 2003.
URL: http://www.wi-fiplanet.com/tutorials/article.php/2148721

19) Wi-Fi Alliance: "Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise", March 2005.

20) "Wi-Fi Protected Access 2 (WPA2) Overview", The Cable Guy, May 2005.

21) "Advanced Encryption Standard Fact Sheet", January 28, 2002.
URL: http://csrc.nist.gov/CryptoToolkit/aes/

22) http://www.ethereal.com/

23) http://dast.nlanr.net/Projects/Iperf/

24) http://jarok.cs.ohiou.edu/software/tcptrace/manual/index.html

25) http://www.snapfiles.com/get/ipsniffer.html

26) http://masaka.cs.ohiou.edu/software/tcptrace/jPlot/

27) http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

28) Marius Milner, "NetStumbler v0.4.0 Release Notes".
URL:
http://downloads.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf

29) Lin Li, Jingsong Xie, Omar M. Ramahi, Michael Pecht, and Bruce Donham: *Airborne Operations of Portable Electronic Devices*, IEEE Antenna's and Propagation Magazine, Vol. 44, No. 4, August 2002.

30) Myron Kayton, Kayton Engineering Company, Santa Monica, CA: *One Hundred Years of Aircraft Electronics*, Journal of Guidance, Control and Dynamics, Vol. 26, No. 2, March-April 2003.

31) Nguyen, T. X.; Koppen, S. V.; Ely, J. J.; Williams R. A.; Smith, L. J., and Salud, M.T.: *Portable Wireless LAN Device and Two-Way Radio Threat Assessment for Aircraft Navigation Radios,* NASA/TP-2003-212438, July 2003.

32) Nguyen, T. X.; Koppen, S. V.; Ely, J. J.; Williams R. A.; Smith, L. J., and Salud, M. T.: *Portable Wireless LAN Device and Two-Way Radio Threat Assessment for Aircraft Navigation Radios,* NASA/TP-2003-213010, March 2004.

33) Jay J. Ely, NASA Langley Research Center: *Electromagnetic Interference to Flight Navigation and Communication Systems: New Strategies in the Age of Wireless*, AIAA Guidance, Navigation, and Control Conference and Exhibit, San Francisco, California, 15-18 August 2005.

34) Mustafa Ergen: *IEEE 802.11 Tutorial*, June 2002.

35) Frank L. Whetten, Andrew Soroker, Dennis A. Whetten, Embry Riddle Aeronautical University, Prescott, Arizona and John H. Beggs, Langley Research Center, Hampton, Virginia: *Wireless Local Area Network Performance Inside Aircraft Passenger Cabins.*

36) Feng Li, Mingze Li, Huahui Wu, Mark Claypool and Robert Kinicki: *Tools and Techniques for Measurement of IEEE 802.11 Wireless Networks.*

37) Jangeun Jun, Pushkin Peddabachagari, Mihail Sichintiu: *Theoretical Maximum Throughput of IEEE 802.11 and its Applications.*

38) http://www.nts.ku.edu/services/data/networkmgmt/wireless/802_11frequency.jsp.

39) "Fly-by-Wireless": A Revolution in Aerospace Vehicle Architecture for Instrumentation and Control, Abstract Draft, February 2006, NASA/JSC/George Studor.

40) http://www.securaplane.com/pdf/st3000.pdf

41) Hayward, R., Marchick, A., Powell, J. D., "Single Baseline GPS Based Attitude Heading Reference System (AHRS) for Aircraft Applications," Proceedings of the 1999 American Control Conference, Volume 5, p.3655 – 3659.

42) "NAV420CA Series User's Manual," Document 7430-0121-03, Revision B, February 2007.

43) http://www.ads-b.com/home.html.

44) http://www.ampro.com/index_interactive_GIF.asp.

45) http://www.mesanet.com/adapterinfo.html.

46) http://www.tri-m.com/.

47) http://www.hyperlinktech.com/.

48) http://www.diamondsystems.com/.

49) http://www.lantronix.com/device-networking/external-device-servers/wibox.html.

50) http://www.pcavionics.com/features.jsp.

51) Robert J. Hooper, Todd K. Sprague: *MountainScope User Guide*, Revision 6, 2004.

52) Jay Hendrix, Jeff Raimo, *Wireless 101: A look at a leading-edge technology*, Siemens Building Technologies, Inc.

Appendix A

Analysis of IEEE 802.11a/b/g Protocol Robustness for Essential Data Applications

Flight Test 01- Safety Report

(Revision A)

Flight Experiment:	Performance Demonstration of Wireless Avionics System	
Date:	26 November, 2007	
Submitted by:	Satish Chilakala,	Flight Test Engineer
	Pradeep Attalury,	Vehicle/Instrumentation Engineer
	Ron Renz,	Test Pilot

David R. Downing for

Dr. Richard Colgren
Department Representative

Charge to the Safety Board

The University of Kansas, Aerospace Engineering Department asks that you review this Safety Document relative to the safety of operation. Your signature approving this plan only indicates that in your judgment operation is safe.

Thank you for your willingness to share your unique expertise.

Dr. Richard Colgren

Safety Board Certification

Signature: Richard Colgren

Print Name: Richard Colgren

Signature: David R. Downing

Print Name: David Downing

Signature: ______________________________

Print Name: ____________________________

Revisions:

Date Submitted

Original Document: .... **Date: _11/19/07_**

Rev. A .... **Date: _11/26/07_**

Rev. B .... **Date: _________**

Rev. C .... **Date: _________**

Rev. D .... **Date: _________**

Table of Contents:

Test Overview

The purpose of the flight test described in this document is to demonstrate the performance of a two node wireless avionics network. The two node network is connected wirelessly by the IEEE 802.11g link that is established using the WiBox wireless device server. Of the two nodes, one is a sensor node that incorporates a GPS and an Attitude, Heading Reference System (AHRS). The other node is a Cockpit Display Unit consisting of a rugged laptop with MountainScope software for display of the aircraft's attitude, location, and graphical terrain information. It would also have the NAV-VIEW software for displaying the attitude of the aircraft. The performance of the wireless network during the flight will be monitored and recorded by software installed on the laptop.

During the flight test, no data from the onboard instruments will be recorded. The attitude and navigational data from the NAV420 will be logged into the laptop during the aircraft's maneuvers. The data logging will be done at 100 Hz. As there are no wires involved in connecting the sensor node with the display node, the installation of the test equipment is simple and does not require any aircraft modifications. This would demonstrate the advantages to using wireless technology for both flight testing and as an onboard avionics system.

Test Objectives

The objective of this flight test is to demonstrate and evaluate the performance of the two node wireless avionics network. This would be done by flying the aircraft along a determined course involving standard maneuvers: climb, cruise, turn, flight control doublets, flight control impulses, flight control frequency sweeps, and descent. This requires the pilot to fly the flight cards in this document.

The objective of the flight test is the establishment of the performance of the wireless network and to gain insight into its performance in terms of accuracy and network availability in actual flight conditions. These conditions consist of standard maneuvers.

Proposed Schedule

The flight test has been scheduled for the week of 26 November 2007. Flight tests can be carried out any time between dawn and dusk during this period, depending on the availability of the team members and the aircraft during suitable weather conditions.

Operational Limits

The operational limits for the airplane are as follows:

- Maximum Takeoff Weight: 2,300 lbs (May not be exceeded for any reason.)

- Maximum Speed--V_{NE}: 182 MPH (May not be exceeded at any time.)
- Maximum Structural Cruising Speed--V_{NO}: 145 MPH (Only exceed in smooth air.)
- Minimum Speed (Power off Stall), Clean Configuration--V_{S1}: 57 MPH
- Minimum Speed During Flight Test--$1.3V_{S1}$: 74.1 MPH (Giving a safety factor of 1.3)

Appendix C details the weight and balance data for the aircraft and the planned flight test. A speed envelope of 75 to 110 KIAS is defined for this flight test. The actual flight envelope chosen for this test is given in Appendix D.

Per FAR 91.119, operating limits state:

- Anywhere: An altitude allowing, if a power unit fails, an emergency landing without undue hazard to persons or property on the surface.
- Over congested areas: Over any congested area of a city, town or settlement, an altitude of 1,000 feet above the highest obstacle within a horizontal radius of 2,000 feet.
- Over other than congested areas: An altitude of 500 feet above the surface, except over open water or sparsely populated areas. In those cases, the aircraft may not be operated closer than 500 feet to any person, vessel or structure.

Test Area

The tests described in this document will be performed in the vicinity of Lawrence Municipal Airport (KS) at a distance deemed appropriate by the pilot in command to avoid the local airport traffic.

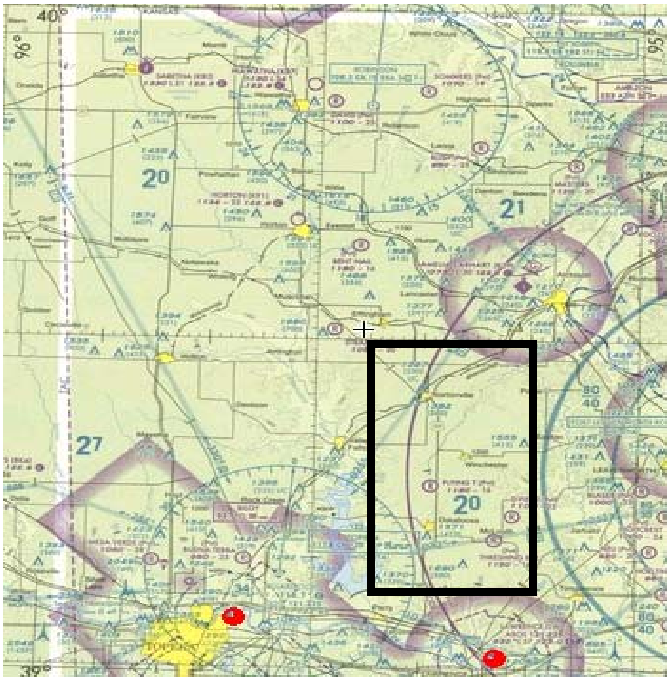


Figure A.1: Test Area

Note: 1. The highest terrain within the Test Area is 550 feet above ground level.

2. The nominal test area extends from N39º10’ to N40 º and from W95 º10’ to W96 º.

Weather Conditions

This flight must occur in VFR flight conditions. The decision on acceptable VFR weather for this flight test is to be made by the pilot.

On-Board Instrumentation Requirements

Data from the EMI test and the entire flight is being recorded. The on-board instrumentation requirements are:

- ➢ Crossbow Technologies’ NAV 420, Attitude, Heading and Reference System (AHRS).
- ➢ Patch Antenna for GPS reception for NAV 420.
- ➢ WiBox serial device server.
- ➢ A 12 Volt 5.0 Amp. Hr Battery, power source for the NAV420 and the WiBox.
- ➢ Toughbook, rugged laptop with MountainScope and NAV-VIEW software installed.

Ground Instrumentation Requirements

The ground instrumentation requirements are – None.

Vehicle Requirements

The vehicle must be capable of the following:

- Carry the pilot and 2 other crewmembers, and sufficient fuel for at least 2.5 hours of flight (1.5 total hour test maximum plus at least 1 hour of safety reserves).
- Be equipped with the instrumentation described above.
- It must be a type of aircraft currently certified by the FAA in the normal aircraft category (FAR Part 23) and have a current Airworthiness Certificate, Registration Certificate, Operating Limitations and Weight and Balance calculations all located on board the aircraft for each flight. Maintenance must have been carried out in accordance to FAR 91.409 (100 -hour inspections) and FAR 91.417 (Annual Inspection).

Proposed Aircraft:

- Type: 172-M
- Registration Number: N12800
- Owner: University of Kansas

This aircraft fulfills the above requirements.

Vehicle Modifications and Special Requirements

The instrumentation required is enclosed within an aluminum box. The box contains the NAV420 and the WiBox. This self-contained box has its own 12 Volt power source and thus no power is required from the aircraft. The system will be located behind the aircraft's cockpit area. There are no aircraft modifications required for this flight test.

Pilot and Crew Requirements

The pilot of the aircraft must have at least a Commercial Pilot's License for the Airplane Single Engine Land category and class. He/She must have a current class II medical exam and have a current biannual flight review within the last 24 months before the flight test date. In addition, he/she must have completed at least three takeoffs and landings within 90 days prior to the flight within the same category and class of aircraft to meet the FAA currency requirements to carry passengers during the daytime.

The flight test crew other than the pilot will consist of two crewmembers that are knowledgeable about the nature of the flight test and their respective tasks. The task description for the two flight test crewmembers is as follows:

Crewmember 1:

- Give pilot instructions for the current flight test point including the flight condition to be in.
- Assist the pilot in observing the surrounding airspace for collision avoidance during the flight test.

Crewmember 2:

- Operate the rugged laptop and log the data for the different test maneuvers through out the flight.
- Operate the test equipment or instrumentation as needed for the flight test.
- Assist the pilot in observing the surrounding airspace for collision avoidance during the flight test.

Ground Support Requirements

Ground support will take place before and after the flight is completed; none will be required during the actual flight tests. Prior to the flight, the team members will carry out their respective responsibilities to ensure that the aircraft is ready for the flight test and that the crewmembers have been properly briefed on the procedures to be carried out. A flow chart of the decision making process is given in Appendix E. The team members have the following positions and responsibilities during ground operations. Appendix F provides checklists for each position.

- Pilot in Command (PIC) – Has ultimate responsibility for the *safety of the flight* and therefore has the final authority in making a go or no-go decision. He is responsible for briefing the other crewmembers on safety and emergency procedures prior to the flight. The PIC is also responsible for performing a pre-flight inspection of the aircraft according to the pre-flight checklist and reviewing the weight and balance calculation to ensure the aircraft is not overweight and that the center of gravity will not be out of range for any portion of the flight.

- Flight Test Engineer (FTE) – Is responsible for making the go or no-go decision for purposes of the *test mission success*. The FTE is responsible for the overall coordination of the flight test operation and team. Therefore, he/she must ensure that the PIC has been properly briefed on the nature and procedures of the flight test. The FTE is also responsible for training and evaluating the other team members in their tasks.

- Vehicle/Instrumentation Engineer (VE) –Assists the PIC in performing the pre-flight preparations of the aircraft. This includes understanding any special limitations of the aircraft, reviewing recent maintenance and repair records, reviewing the squawk list and the status of actions. The VE must ensure that the aircraft is ready for the test flight, and determine if the aircraft is airworthy and ready to perform the required mission. The VE is responsible for the weight and balance calculation of the aircraft and for performing a post-flight inspection of the vehicle and making additions to the squawk list if necessary. Is also responsible for ensuring that the required instrumentation is installed and operational prior to each flight test. He/she has no authority to cancel a flight if an instrument that is vital to the test is not operational, but can advise the FTE to do so. The VE performs a post flight checkout of the instrumentation system and is responsible for the documentation of the system status, including any failure, permanent or intermittent, that may occur.

If at anytime the VE discovers a condition that is unsafe or inadequate for the completion of the flight test, then that team member has the responsibility to notify the PIC and FTE. The PIC and FTE have the authority and responsibility to cancel the flight at any time they believe the flight presents a safety concern, while the FTE may cancel the flight at any time he/she believes the test cannot be successfully completed.

Estimated Cost and Source of Funding

The cost per hour of the Cessna 172 being rented is $100 per hour, including fuel. This flight test will require more than 1.5 aircraft operating hours to complete, therefore the rental cost will not exceed $150. Equipment required for the wireless avionics network have already been acquired and will require no additional funding. The source of funding for the flight test is the Department of Aerospace Engineering, University of Kansas, to be reimbursed by ADMRC 2008 funding.

The detailed budget analysis is as follows:

1. Aircraft rent, with fuel:	$150.00 (1.5 hrs @ $100/hr)
2. Pilot's charges:	$375.00 (5 hrs @ $75/hr)
Total Maximum Test Cost:	$525.00

Appendix A.A: Dance Card

1	EMI Check
A	COMM Check
B	NAV Check
2	Take Off
	Normal Take off 10 deg flap
3	Straight and Level Flight
	Climb to 3000ft
4	Rate 1 Turns
	Flap 0, Altitude 3000ft, Speed 110 mph IAS
A	Left 20° bank, 180° degree heading change
B	Right 20° bank, 180° degree heading change
5	Steep Turn
	Flap 0, Altitude 3000ft, Speed 110 mph IAS
A	Left 45° bank, 180° degree heading change
B	Right 45° bank, 180° degree heading change
6	Short Impulses
	Flap 0, Altitude 3000ft, Speed 110 mph IAS
A	Elevator Up
B	Elevator Down
C	Rudder Left
D	Rudder Right
E	Left Aileron Up
F	Right Aileron Up

7	Control System Doublets
	Flap 0, Altitude 3000ft, Speed 110 mph IAS
A	Elevator Up, Down, Up
B	Elevator Down, Up, Down
C	Rudder Left, Right, Left
D	Rudder Right, Left, Right
E	Aileron Up, Down, Up
F	Aileron Down, Up, Down
8	Sideslip
	Flap 0, Altitude 3000ft, Speed 110 mph IAS
	Wings Level
A	Left Rudder, Command 5° sideslip angle
B	Right Rudder, Command 5° sideslip angle
	Steady heading
C	Left Rudder, Command 5° sideslip angle
D	Right Rudder, Command 5° sideslip angle
9	Slow Flight Turn
	Flap 0, Altitude 3000ft, Speed 75 mph IAS
A	Left 20° bank, 90° degree heading change
B	Right 20° bank, 90° degree heading change

10	Slow Flight
A	Flap 40, Altitude 3000ft, Speed 75mph IAS
B	Flap 30, Altitude 3000ft, Speed 75mph IAS
C	Flap 20, Altitude 3000ft, Speed 75mph IAS
D	Flap 10, Altitude 3000ft, Speed 75mph IAS
E	Flap 0, Altitude 3000ft, Speed 75mph IAS
11	Acceleration
	Flap 0, Altitude 3000ft, Accelerate to a speed 110 mph IAS
12	Frequency Sweeps
	Flap 0, Altitude 3000ft, Speed 110mph IAS
A	Elevator
B	Rudder
C	Aileron
13	Approach and Landing

Appendix A.B: Flight Test Cards

Flight Test Experiment	Wireless Avionics Network Performance Demonstration
Aircraft Model	172 M
N-number of the aircraft	N-12800
Pilot	Ron Renz
Crew 1	Satish Chilakala
Crew 2	Pradeep Attalury
Date	Approx. 28 November 2007

A	Pre-Flight Procedure		
	1	FTE Briefing to Pilot and Crew	
	2	Pilot Safety Briefing to the Crew	
	3	Hobbs Time	
	4	Tach Time	
	5	Check NOTAMS	
	6	Fuel Quantity	
	7	Aircraft Weight	
	8	Crew and Instrumentation weight	
	9	Pre Flight Inspection from Pilot's Manual Check List	

B	Frequencies		
	1	ASOS	121.25
	2	LWC CTAF	12.30
C	Weather Conditions		
	1	Temperature	
	2	Barometric Pressure	
	3	Winds	
	4	Ceiling/ Visibility	
D	Check Off		
	1	Vehicle Engineer	
	2	Flight Test Engineer	
	3	Pilot in Command	

1 EMI Check

Turn on Test equipment

A COMM Check □

Check onboard communication system for interference.

B NAV Check □

Check onboard navigation system for interference.

2 Take Off

Normal take off with 10 degree flap. □

3 Straight and Level Flight

Climb to 3000ft pressure altitude, maintain 110 mph IAS. □

4 Rate 1 Turn

Configuration:

Flap: 0 deg.
Altitude: 3000ft
Speed: 110 mph IAS

A Left Turn □

Initiate a Rate 1 turn to the left with a bank angle of 20 +/- 5 degrees. Continue the turn thru 180 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

B Right Turn □

Initiate a Rate 1 turn to the right with a bank angle of 20 +/- 5 degrees. Continue the turn thru 180 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

5 Steep Turn

Configuration:

Flap: 0 deg.
Altitude: 3000ft
Speed: 110 mph IAS

A Left Turn □

Initiate a Steep turn to the left with a bank angle of 45 +/- 5 degrees. Continue the turn thru 180 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

B Right Turn □

Initiate a Steep turn to the right with a bank angle of 45 +/- 5 degrees. Continue the turn thru 180 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

6 Short Impulses

Configuration

Flap: 0 deg.
Altitude: 3000ft
Speed: 110 mph IAS

A Elevator Up □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

B Elevator Down □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

C Rudder Left □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

D Rudder Right □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

E Left Aileron Up □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

F Right Aileron Up □

Wings level, stabilize airplane, give a short impulse of approximately 0.25 of the control over 1 sec. Allow airplane to settle before the next maneuver.

7 Control System Doublets

Configuration

Flap:	0 deg.
Altitude:	3000ft
Speed:	110 mph IAS

A Elevator Up Down Center □

Wings level, stabilize the airplane. Apply approximately 0.25 elevator input for 2 sec UP and same input for 2 sec DOWN and return to center.

B Elevator Down Up Center □

Wings level, stabilize the airplane. Apply approximately 0.25 elevator input for 2 sec DOWN and same input for 2 sec UP and return to center.

C Rudder Left Right Center □

Wings level, stabilize the airplane. Apply approximately 0.25 LEFT rudder input for 2 sec and same RIGHT rudder input for 2 sec and return to center.

D Rudder Right Left Center □

Wings level, stabilize the airplane. Apply approximately 0.25 RIGHT rudder input for 2 sec and same LEFT rudder input for 2 sec and return to center.

E Aileron Left Right Center □

Wings level, stabilize the airplane. Apply approximately 0.25 LEFT aileron input for 2 sec and same RIGHT aileron input for 2 sec and return to center.

F Aileron Right Left Center □

Wings level, stabilize the airplane. Apply approximately 0.25 RIGHT aileron input for 2 sec and same LEFT aileron input for 2 sec and return to center.

8 Sideslip

Configuration

Flap: 0 deg.
Altitude: 3000ft
Speed: 110 mph IAS

A Wings Level - Left Sideslip □

Wings level, hold LEFT rudder to command LEFT 5 deg sideslip angle.

B Wings Level - Right Sideslip □

Wings level, hold RIGHT rudder to command RIGHT 5 deg sideslip angle.

C Steady Heading - Left Sideslip □

Hold LEFT rudder, command LEFT 5 deg sideslip angle, maintaining steady heading during the entire maneuver using roll command as required.

D Steady Heading - Right Sideslip □

Hold RIGHT rudder, command RIGHT 5 deg sideslip angle, maintaining steady heading during entire maneuver using roll command as required.

9 Slow Flight Turn

Configuration:

Flap: 0 deg.
Altitude: 3000ft
Speed: 75 mph IAS

A Left Turn □

Decelerate to 75 mph, stabilize the aircraft. Initiate a Rate 1 turn to the LEFT with a bank angle of 20 +/- 5 degrees. Continue the turn thru 90 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

B Right Turn □

Initiate a Rate 1 turn to the RIGHT with a bank angle of 20 +/- 5 degrees. Continue the turn thru 90 degrees maintaining airspeed +/- 10 mph IAS. Maintain altitude +/- 100ft.

10 Slow Flight

A Configuration: □

Flap:	40 deg.
Altitude:	3000ft
Speed:	75 mph IAS

Hold heading, wings level, set flaps to 40 deg, maintain airspeed +/- 10 mph IAS, maintain altitude +/- 100ft.

B Configuration: □

Flap:	30 deg.
Altitude:	3000ft
Speed:	75 mph IAS

Hold heading, wings level, retract the flaps to 30 deg, maintain airspeed +/- 10 mph IAS, maintain altitude +/- 100ft.

C Configuration: □

Flap:	20 deg.
Altitude:	3000ft
Speed:	75 mph IAS

Hold heading, wings level, retract the flaps to 20 deg, maintain airspeed +/- 10 mph IAS, maintain altitude +/- 100ft.

D Configuration: □

Flap:	10 deg.
Altitude:	3000ft
Speed:	75 mph IAS

Hold heading, wings level, retract the flaps to 10 deg, maintain airspeed +/- 10 mph IAS, maintain altitude +/- 100ft.

E Configuration: □

Flap:	0 deg.
Altitude:	3000ft
Speed:	75 mph IAS

Hold heading, wings level, retract the flaps to 0 deg, maintain airspeed +/- 10 mph IAS, maintain altitude +/- 100ft.

11 Acceleration

Configuration: □

Flap:	0 deg.
Altitude:	3000ft
Speed:	110 mph IAS

Accelerate to 110 mph IAS, stabilize, hold heading, keep wings level.

12 Frequency Sweeps

Configuration:

Flap: 0
Altitude: 3000ft
Speed: 110 mph IAS

A Elevator □

Apply elevator chirp (increasing frequency sine wave, starting at approximately 1 cycle over 5 seconds to 2 cycles in 1 second) input of approximately 0.25 of the control magnitude. On completion return control to center, holding the heading and maintaining airspeed +/- 10 mph IAS, and maintaining altitude +/- 100 feet.

B Rudder □

Apply rudder chirp (increasing frequency sine wave) input of approximately 0.25 of the control magnitude. On completion return control to center, holding the heading and maintaining airspeed +/- 10 mph IAS, and maintaining altitude +/- 100 feet.

C Aileron □

Apply aileron chirp (increasing frequency sine wave) input of approximately 0.25 of the control magnitude. On completion return control to center, holding the heading and maintaining airspeed +/- 10 mph IAS, and maintaining altitude +/- 100 feet.

13 Approach and Landing

Return to the airport □

Post-Flight Procedure

1. Hobbs Time ____________________

2. Tach Time ____________________

Appendix A.C: Weight and Balance

Figure A.C1 illustrates the Cessna 172P center of gravity envelope and the flight test center of gravity range within that envelope. The following data was used to generate the c.g. moment envelope shown in Figure A.C1.

Empty Weight (includes oil, fixed equipment, and unusable fuel)	1,429.8lbs
Full Fuel (42 gal at 6 lbs/gal)	252 lbs
Pilot	170 lbs
Crew 1 (Front seat)	130 lbs
Crew 2 (Rear seat)	180 lbs
Maximum Takeoff Weight	2,300 lbs

*Clipboards, pencils, stopwatches, and other such items are included in crew weight.

Table A.C1: Takeoff Weight and Balance

Component	Weight (lbs)	Arm (in)	Moment (in-kips)
Empty Wt	1429.8	39.13	55.95
Max Fuel	252	46.0	11.59
Pilot	170	37.0	6.29
Crew 1	130	37.0	4.81
Crew 2	180	73.0	13.14
Ewuipment	20	123.0	2.46
Totals:	2181.8		94.24

Table A.C1 shows that the takeoff weight is 2,181.8 lbs and the center of gravity is located at 43.2 inches. Figure A.C2 indicates that the forward c.g. limit is 83 in-kips or 37.5 inches, and the aft c.g. limit is 105 in-kips or 47.5 inches.

The worst case assumes the flight will burn all of its fuel, less the day VFR reserves of 30 minutes, or about 25.2 lbs of fuel, as is illustrated in Table A.C2.

Table A.C2: Landing Weight and Balance

Component	Weight (lbs)	Arm (in)	Moment (in-kips)
Empty Wt	1429.8	39.13	55.95
Min Fuel	25.2	46.0	1.16
Pilot	170	37.0	6.29
Crew 1	130	37.0	4.81
Crew 2	180	73.0	13.14
Equipment	20	123.0	2.46
Totals:	1955		83.81

Table A.C2 shows that the minimum fuel landing weight is 1,955 lbs and the c.g. is located at 42.9 inches, Figure A.C2 indicates that the forward c.g. limit is 70 in-kips or 35.3 inches, and the aft c.g. limit is 93.5 in-kips or 39.7 inches.

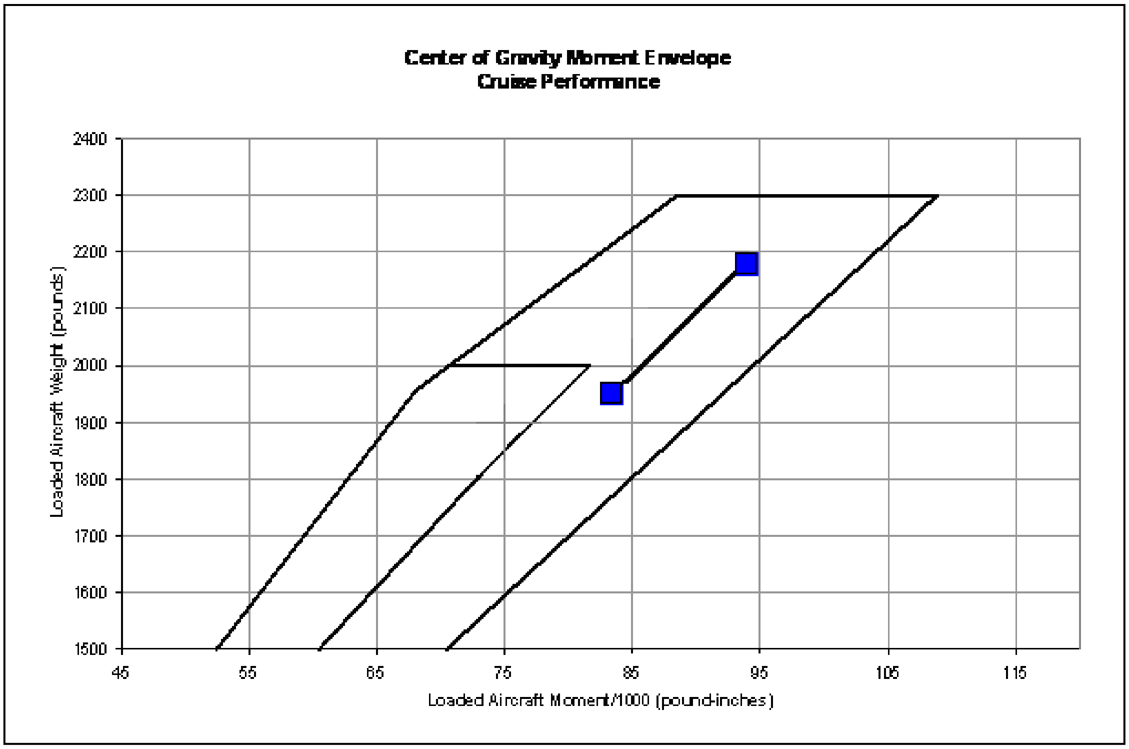


Figure A.C-1: Center of Gravity Moment Envelope

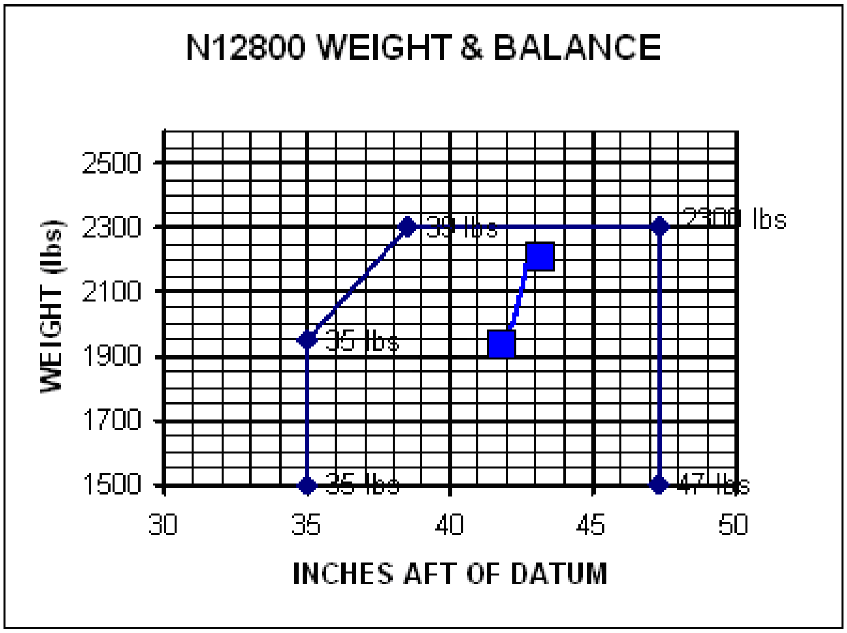


Figure A.C-2: N12800 Weight and Balance

Appendix A.D: Flight Envelope

Figure A.C1 illustrates the Cessna 172M flight envelope and the planned flight test envelope. The following data was used to generate Figure A.C1.

Minimum Test Altitude	1,000 ft AGL
Maximum Test Altitude	2,500 ft MSL
Minimum Test Speed	75 MPH
Maximum Test Speed	121 MPH
Maximum Sustained Flight Altitude	12,500 ft MSL
Minimum Flight Altitude (other than landing approach)	500 ft AGL
Stall Speed (Level Flight, Max Gross Wt, Flaps Up) --V_{S1}	57 MPH
Maximum Structural Cruising Speed (Max Gross Wt)--V_{NO}	145 MPH
Maximum Maneuvering Speed (2400 lbs)--V_A	112 MPH
Maximum Maneuvering Speed (2000 lbs)--V_A	106 KIAS

Risk Assessment:

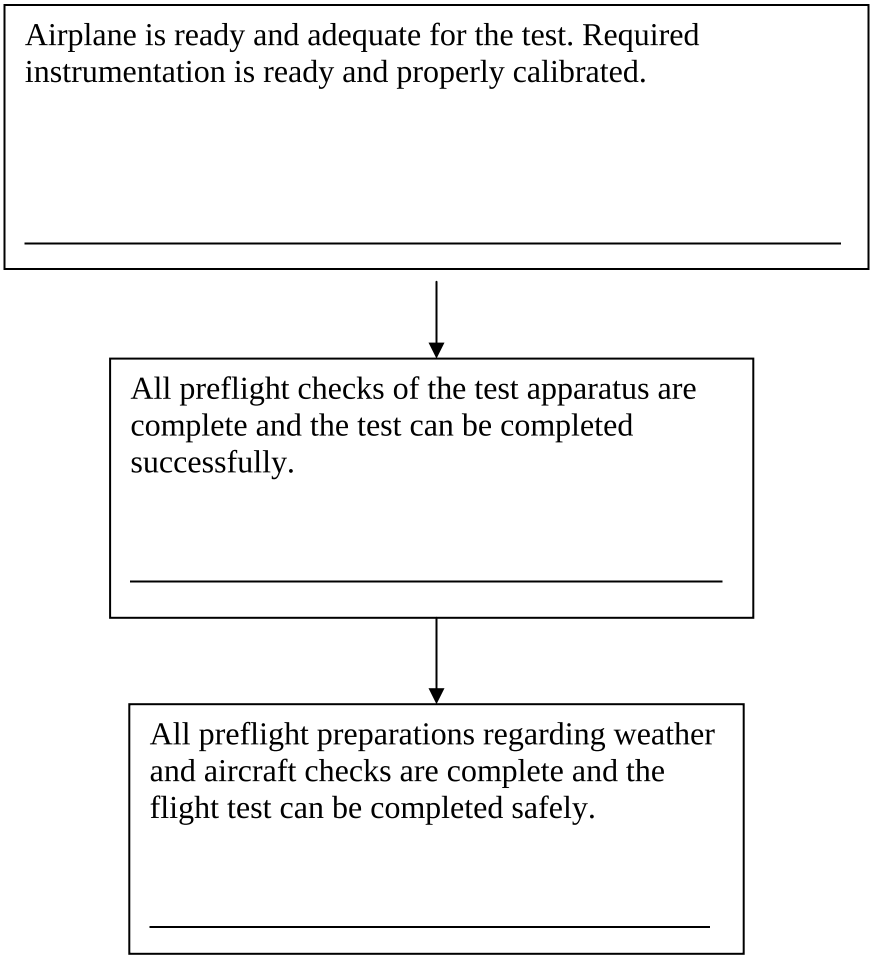
Since the flight envelope and the weight and c.g. limits of the test aircraft will not be exceeded during the specified test flight, and no modifications are being made to the aircraft and its systems, this flight test is classified as low risk.

Conformity Inspection Requirements:

No modifications will be made to the aircraft as built to the type certificate; therefore, no conformity inspections are required.

Appendix A.E: Flow Chart

This flow chart illustrates the preflight process and the authority of each individual.



Airplane is ready and adequate for the test. Required instrumentation is ready and properly calibrated.

____

All preflight checks of the test apparatus are complete and the test can be completed successfully.

____

All preflight preparations regarding weather and aircraft checks are complete and the flight test can be completed safely.

____

Appendix A.F: Personnel Checklists:

The following two checklists detail the duties of each individual and must be completed prior to conducting the flight test. The pilot is to use the checklist for the aircraft.

Flight Test Engineer:

Vehicle Engineer checklist reviewed □

Vehicle as signed off by Vehicle Engineer is ready for the test. □

Instrumentation Engineer checklist reviewed □

The instrumentation as signed off by the Instrumentation Engineer is adequate and ready for the test. □

Instrumentation has been implemented to the vehicle in a proper fashion. □

Pilot has been briefed about his tasks during the test □

Data Processing Engineer has been briefed about his tasks during the test □

Test status: **Go** □ **Cancel** □

______________________________ Flight Test Engineer

____________ Date

Vehicle/Instrumentation Engineer:

Aircraft scheduled for test times. □

All aircraft documentation is on board □

Airworthiness Certificate □

Registration Card □

Operations Manual □

Weight and Balance Data □

Rugged Laptop, charged completely and installed with all the required software □

WiBox functional and set to go. □

NAV420 functional and set to go □

GPS antenna connected to NAV420 and set to go □

Fuel Tanks Full □

____ _____________

Vehicle/Instrumentation Engineer Date

Appendix B: Flight Test Maneuvers

This section gives the results of various flight maneuvers, continued from Chapter 5. The take off and Rate 1 turn to the left were mentioned in the section 5.3. Many packet drops were observed during the Rate 1 turn to the left (Figures 5-23 and 5-24). Many unwanted connections were observed during that particular maneuver (Figure 5-32). This maneuver was repeated at a different location (Figure 5-25 and 5-26). During approach and landing (Figures 5-27 and 5-28), there was a loss of connection for about 15 seconds.

Figures B.1 and B.2 show the flight track of the Rate 1 turn to the right and the corresponding plot drawn using MATLAB. A standard rate 1 turn takes about 2 minutes to complete a 360^o heading change. The maneuver was conducted at 3,000 ft altitude and 110 mph IAS. It took about 60 seconds to complete a 180^o heading change. There were some packets dropped for about 4 seconds.

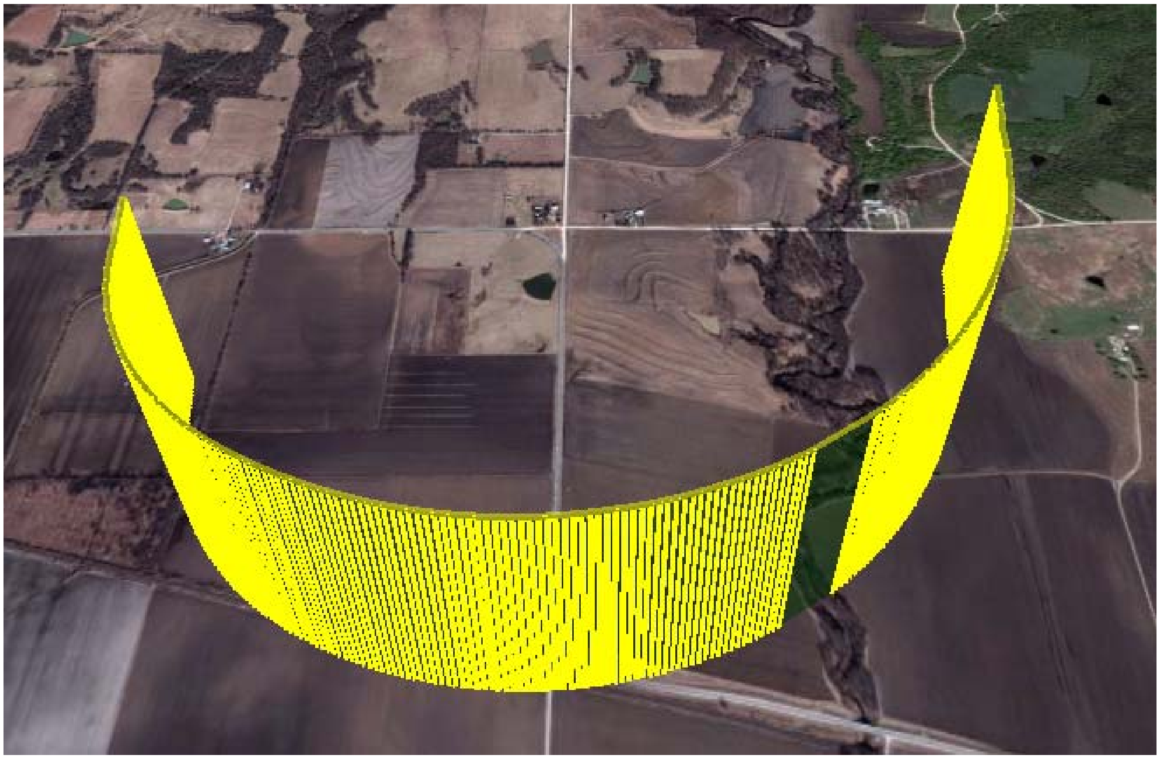


Figure B.1: Google Earth Screenshot of the Rate 1 Turn (Right)

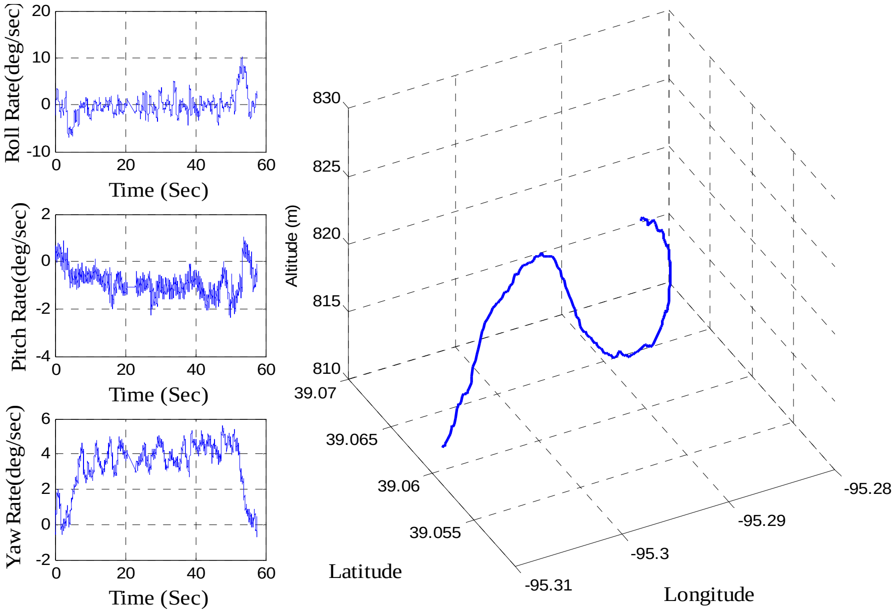


Figure B.2: Rate 1 Turn (Right)

Figure B.3 shows the flight track of the steep turn to the left and right. Figures B.4 and B.5 show the corresponding results drawn using MATLAB. The maneuver was conducted with a bank angle of 45 +/- 5 degrees, at 3,000 ft and 110 mph IAS. It took 60 seconds for both the left and right turn maneuvers. During the right turn, multiple packet losses were observed.

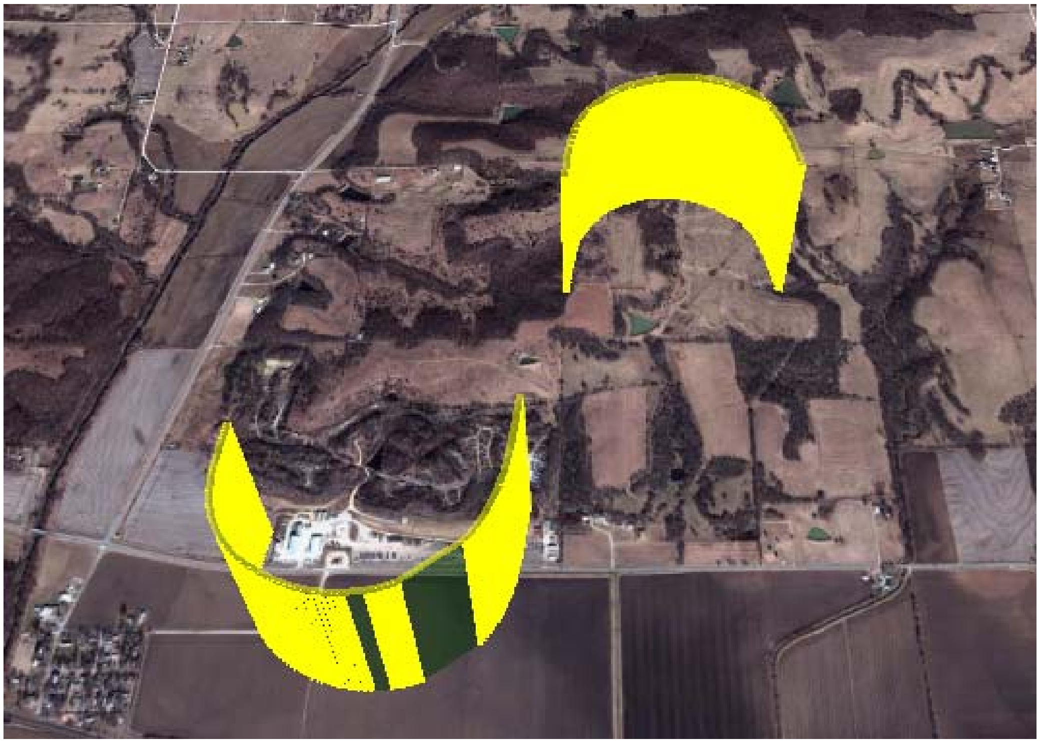


Figure B.3: Google Earth Screenshot of the Steep Turn (Left & Right)

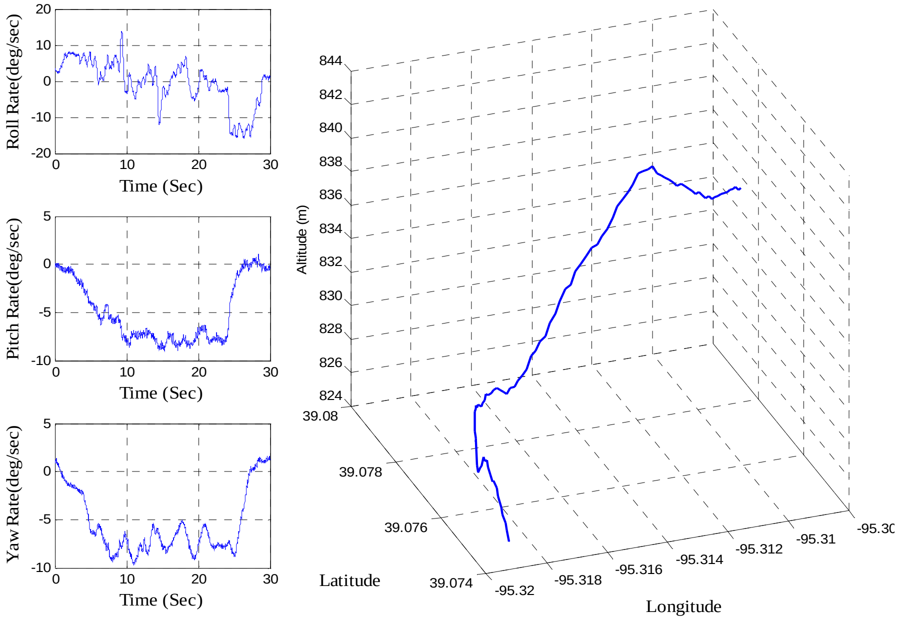


Figure B.4: Steep Turn (Left)

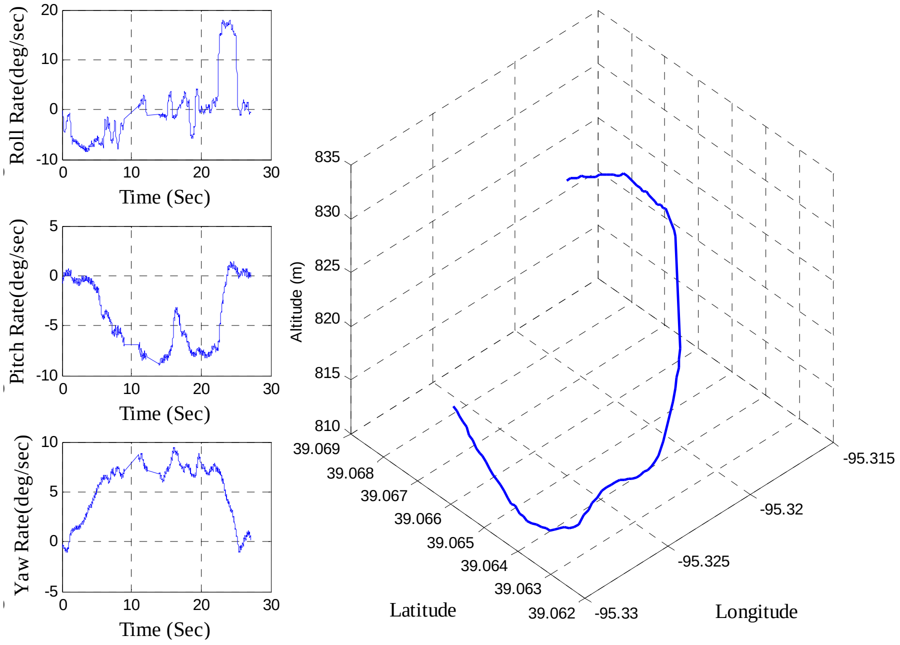


Figure B.5: Steep Turn (Right)

Figures B.6 and B.7 show the flight track and MATLAB results during short duration impulse command to the elevator. The pilot has commanded approximately 15% of the maximum elevator deflection for 1 second. The data from the sensor was recorded in a single file for both elevator up and down commands. Note that the observed gap in Figure B.6 is not due to data loss. It is due to the pause between the two short elevator impulse tests (i.e., between the elevator up and elevator down commands).

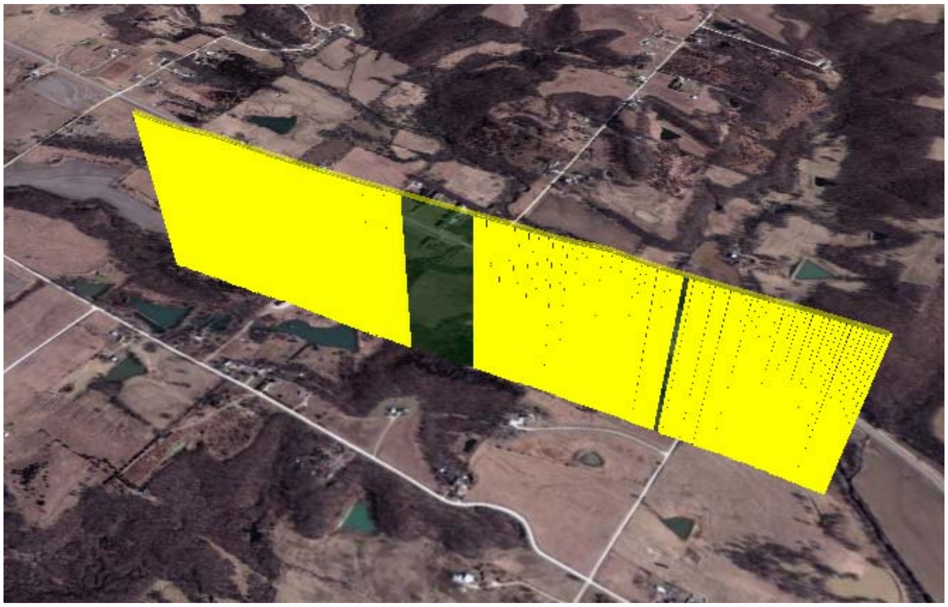


Figure B.6: Google Earth Screenshot of the Short Impulses (Elevator)

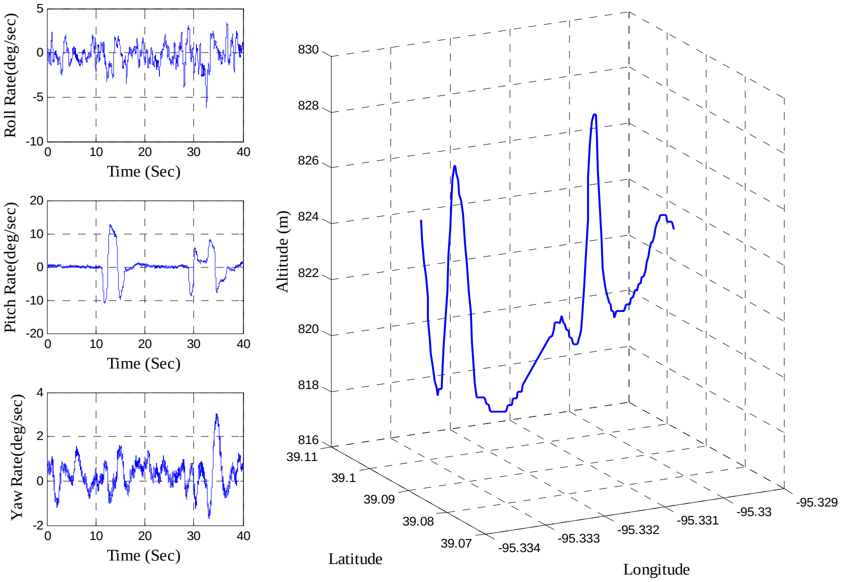


Figure B.7: Short Impulses (Elevator)

Figures B.8 and B.9 show the flight track and the MATLAB results during short impulse command to the rudder. The pilot has commanded approximately 25% of the maximum rudder deflection for 1 second. It took 30 seconds for the maneuver. The data from the sensor was recorded in a single file for both rudder left and right commands. No data loss was observed during this maneuver.

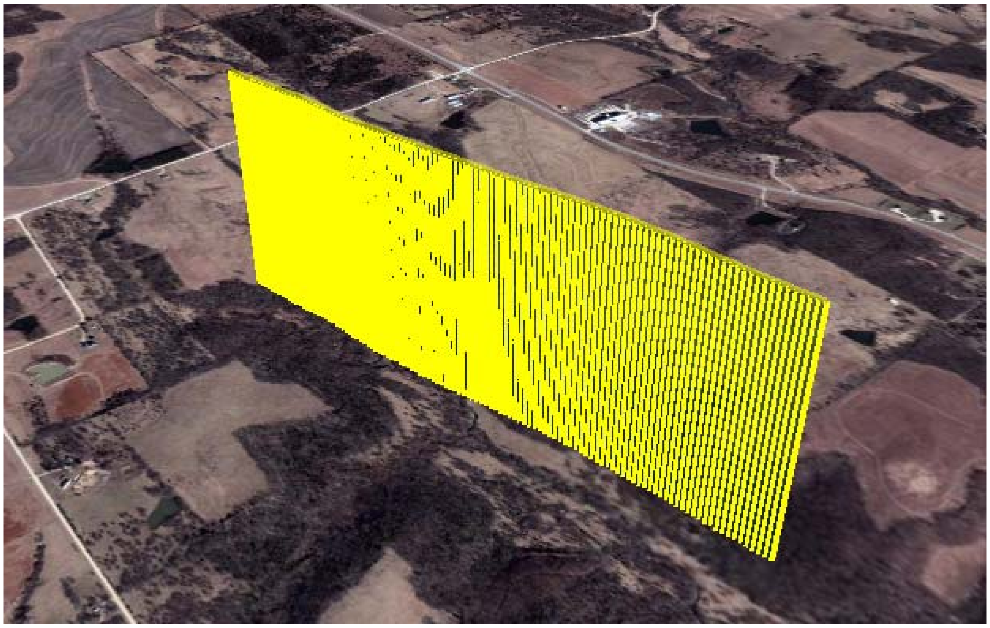


Figure B.8: Google Earth Screenshot of the Short Impulses (Rudder)

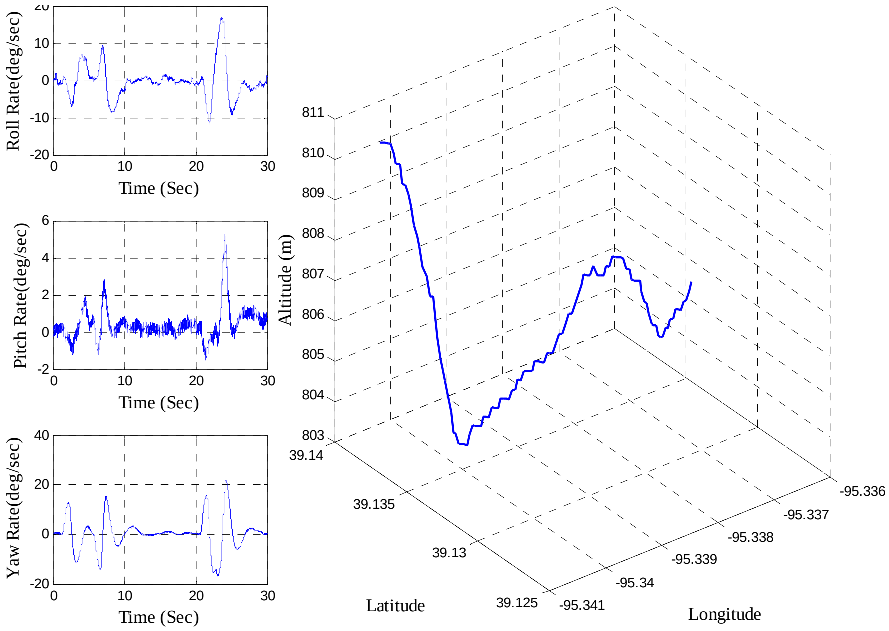


Figure B.9: Short Impulses (Rudder)

Figures B.10 and B.11 show the flight track and the MATLAB results for a short duration impulse command to the aileron. The pilot has commanded approximately 25% of the maximum aileron control input for 1 second. The data from the sensor was recorded in a single file for both right turn and left turn aileron commands. No data loss was observed during this maneuver.

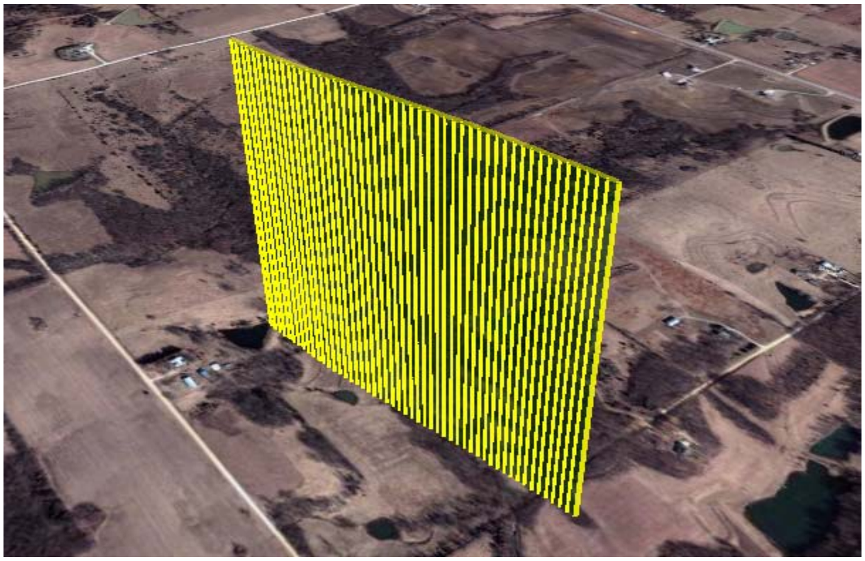


Figure B.10:Google Earth Screenshot of the Short Impulses (Aileron)

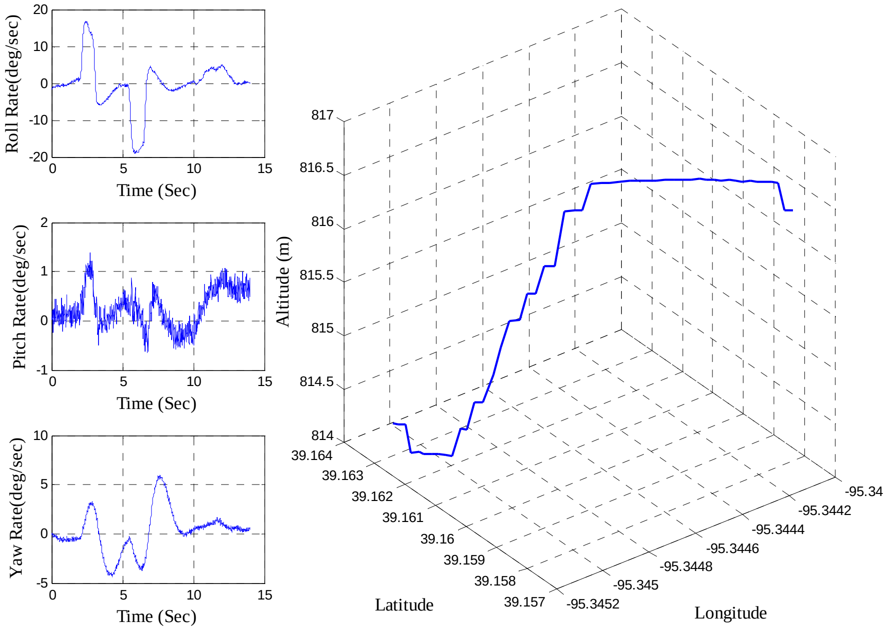


Figure B.11: Short Impulses (Aileron)

Figures B.12 and B.13 show the flight track and MATLAB results from an elevator doublet. The pilot has commanded approximately 25% of the maximum elevator deflection for 2 seconds up, followed by 2 seconds down with a return to center. The order was reversed and the data was logged in the same file. No data loss was observed during this maneuver.

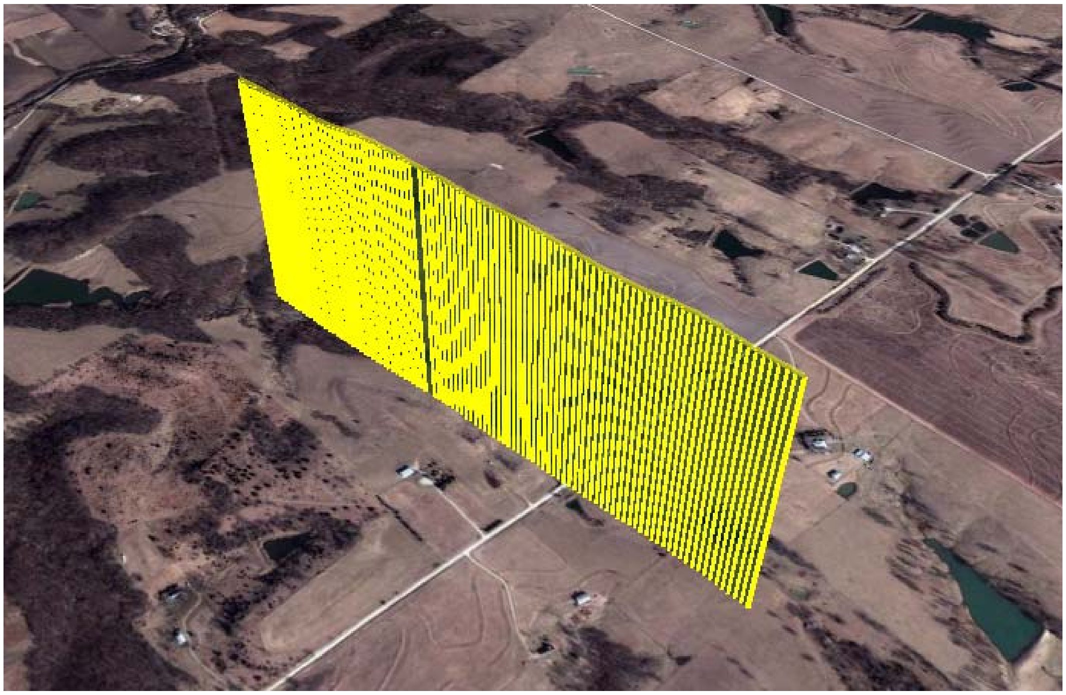


Figure B.12: Google Earth Screenshot of the Elevator Doublets

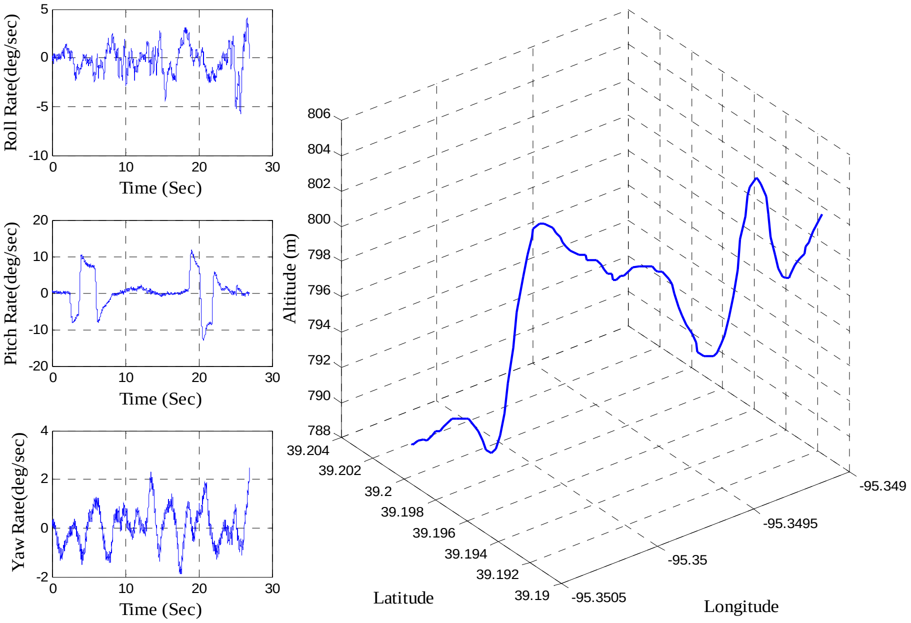


Figure B.13: Elevator Doublets

Figures B.14 and B.15 show the flight track and MATLAB results from an elevator doublet. The pilot has commanded approximately 25% of the maximum rudder deflection for 2 seconds to the left, followed by 2 seconds to the right with a return to center. The order was reversed and the data was logged in the same file. No data loss was observed during this maneuver.

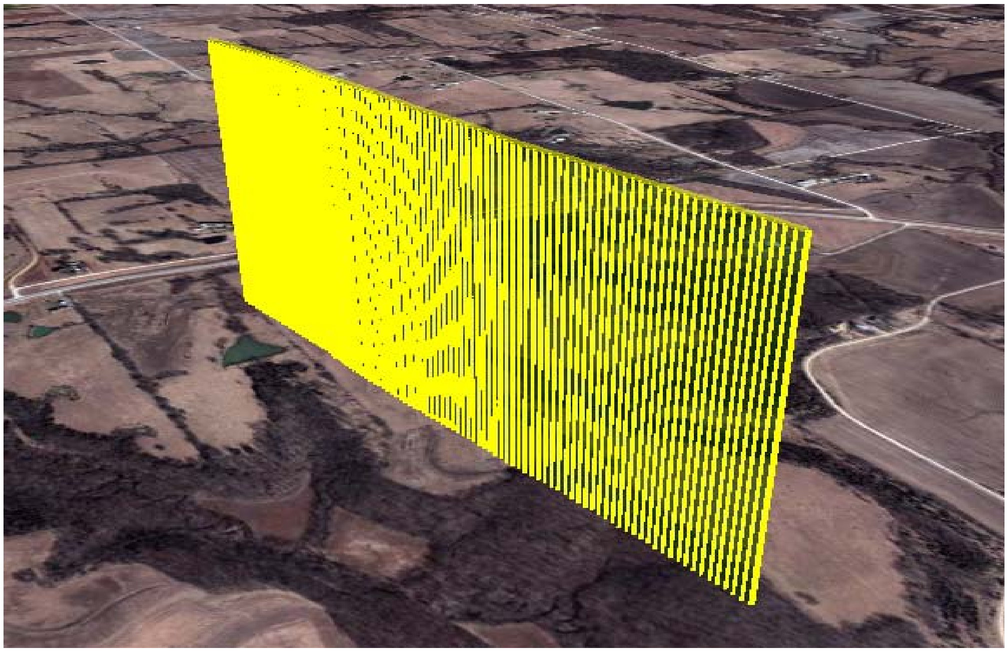


Figure B.14: Google Earth Screenshot of the Rudder Doublets

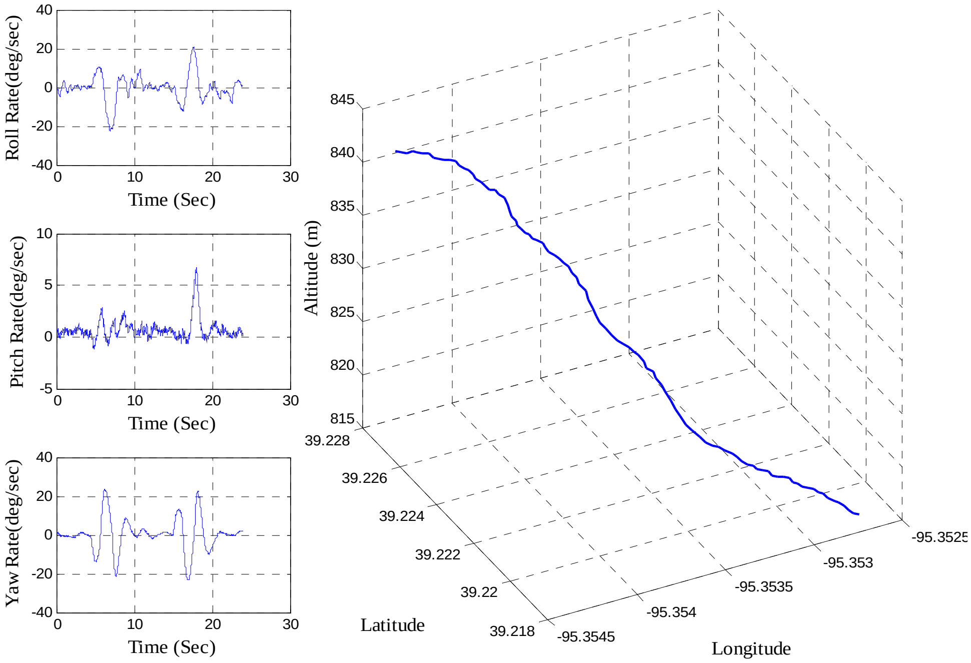


Figure B.15: Rudder Doublets

Figures B.16 and B.17 show the flight track and MATLAB results from an aileron doublet. The pilot has commanded approximately 25% of the maximum elevator deflection for 2 seconds, followed by the opposite command for 2 seconds with a return to center. The order was reversed and the data was logged in the same file. No data loss was observed during this maneuver.

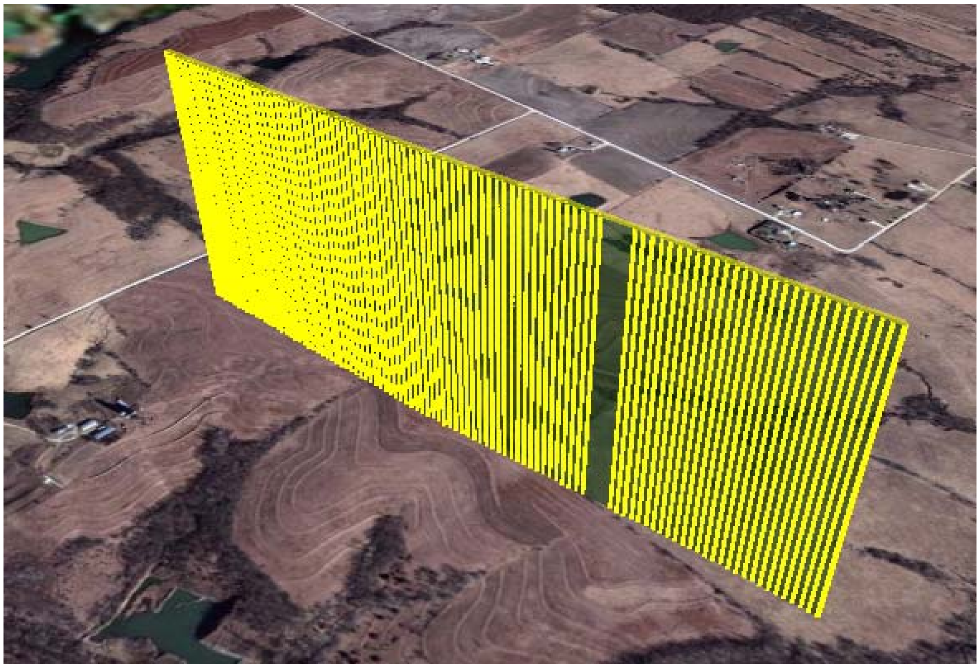


Figure B.16: Google Earth Screenshot of the Aileron Doublets

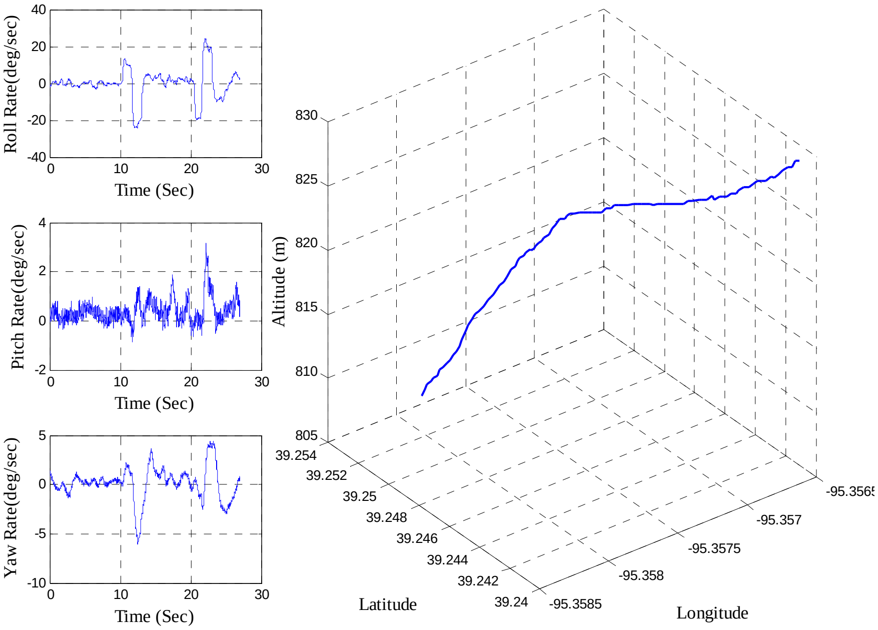


Figure B.17: Aileron Doublets

Figures B.18 and B.19 show the flight track and MATLAB results from a wings level sideslip maneuver. A 5 degree sideslip angle was generated by holding first a left then a right rudder. The maneuver took 31 seconds. No data loss was observed during this maneuver.

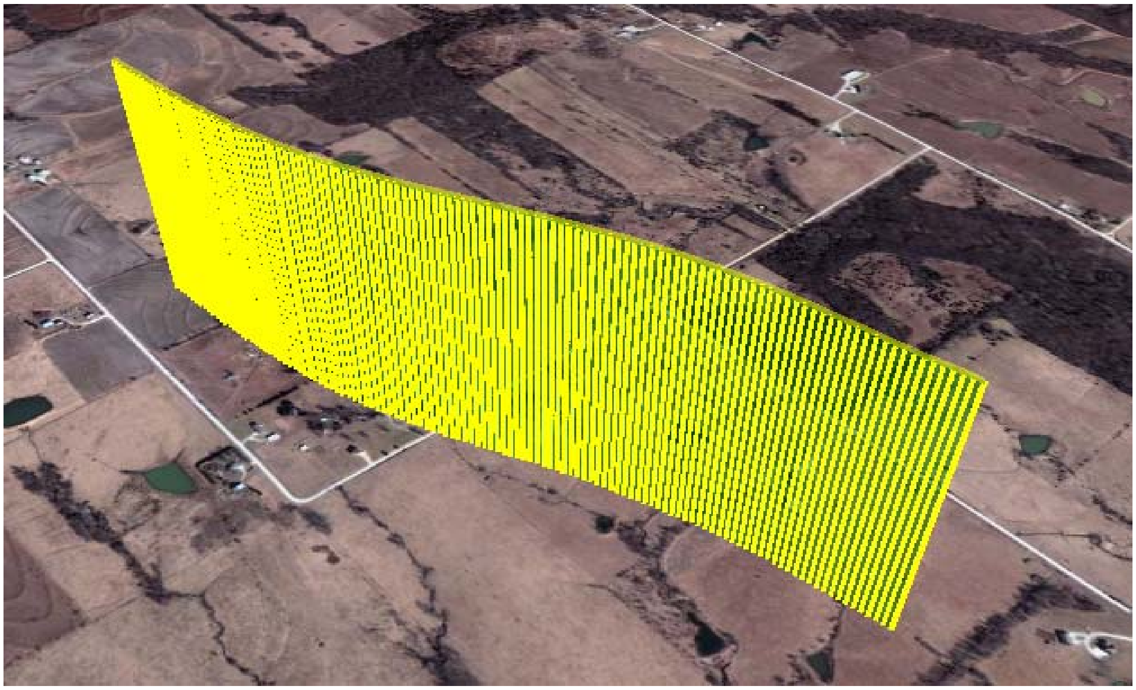


Figure B.18: Google Earth Screenshot of the Wings Level Sideslip

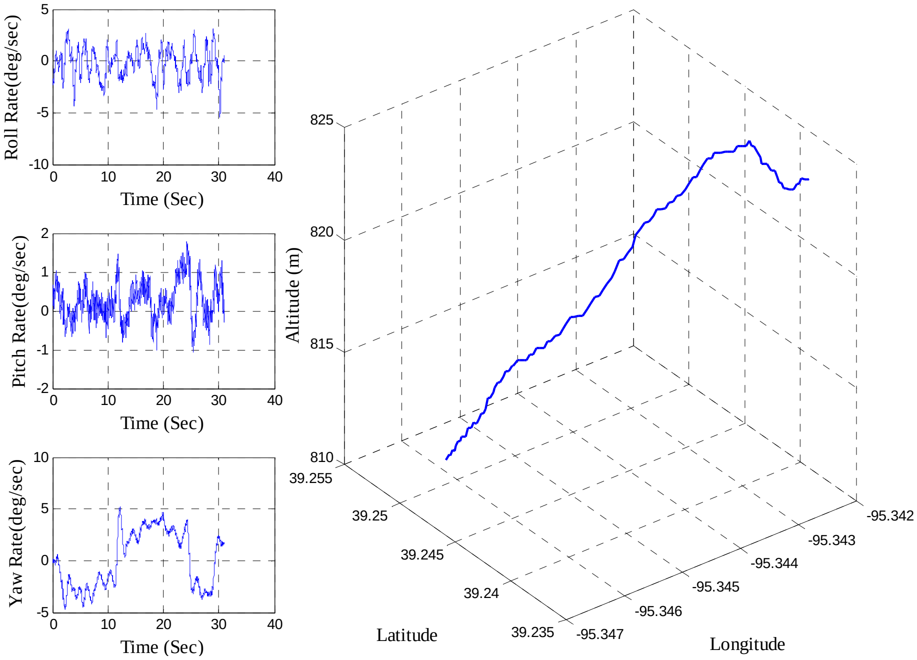


Figure B.19: Wings Level Sideslip

Figures B.20 and B.21 show the flight track and MATLAB results during steady heading sideslip maneuver. A 5 degree left then a right sideslip angle command was given maintaining a steady heading. The maneuver took 45 seconds. No data loss was observed during this maneuver.

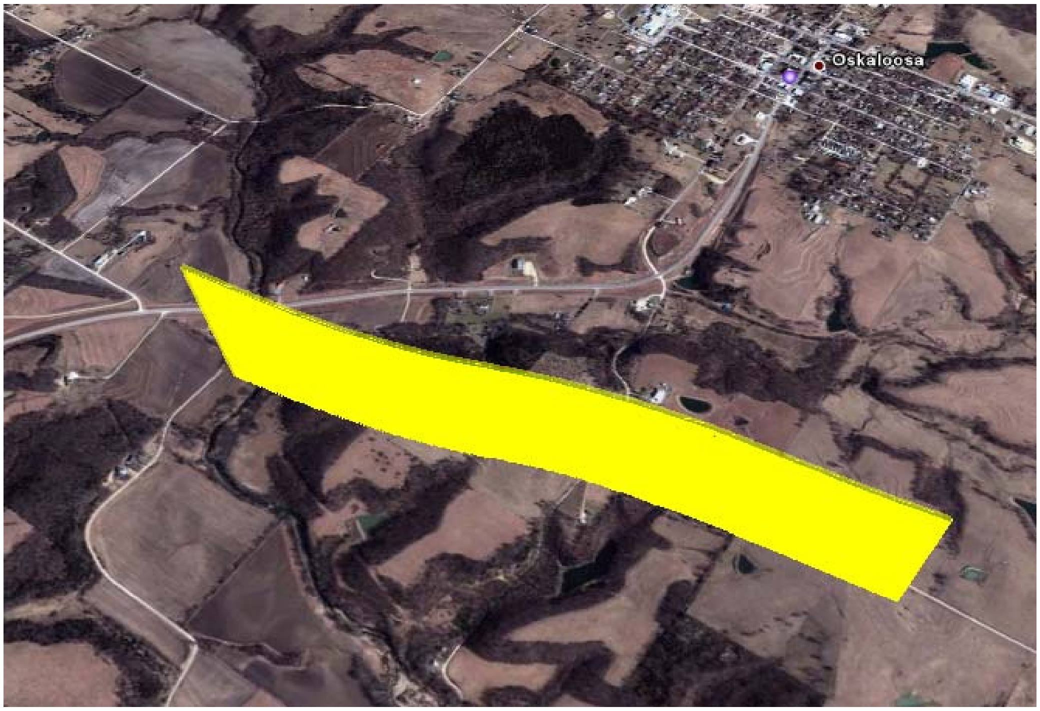


Figure B.20: Google Earth Screenshot of the Steady Heading Sideslip

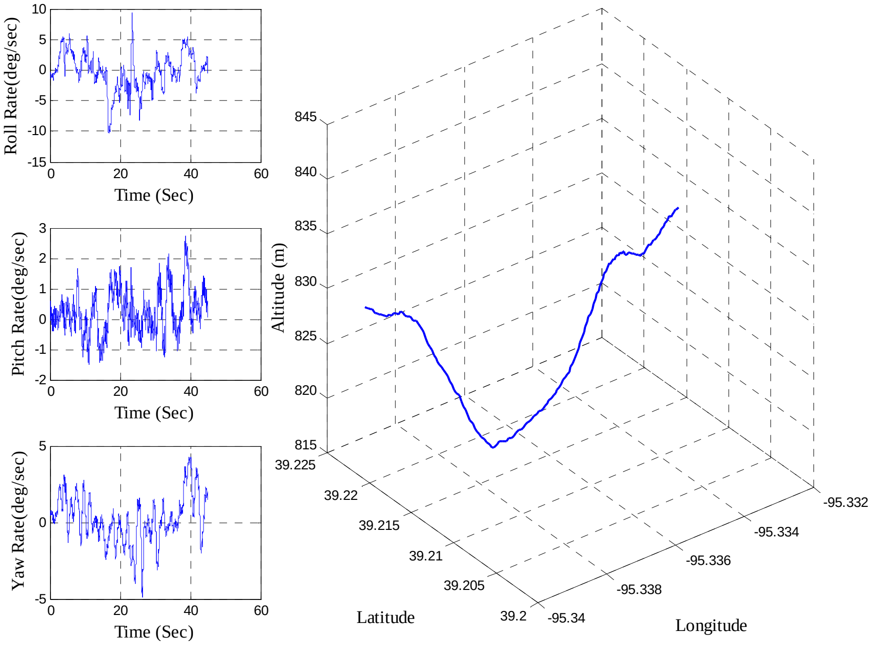


Figure B.21: Steady Heading Sideslip

Figures B.22 and B.23 show the slow flight turn to the left and then the right. The maneuver took about 70 seconds for both the left right turns. The gap shown in Figure B.22 was due to the pause between the different maneuvers (the left and right turns). No packet losses were observed during this maneuver.

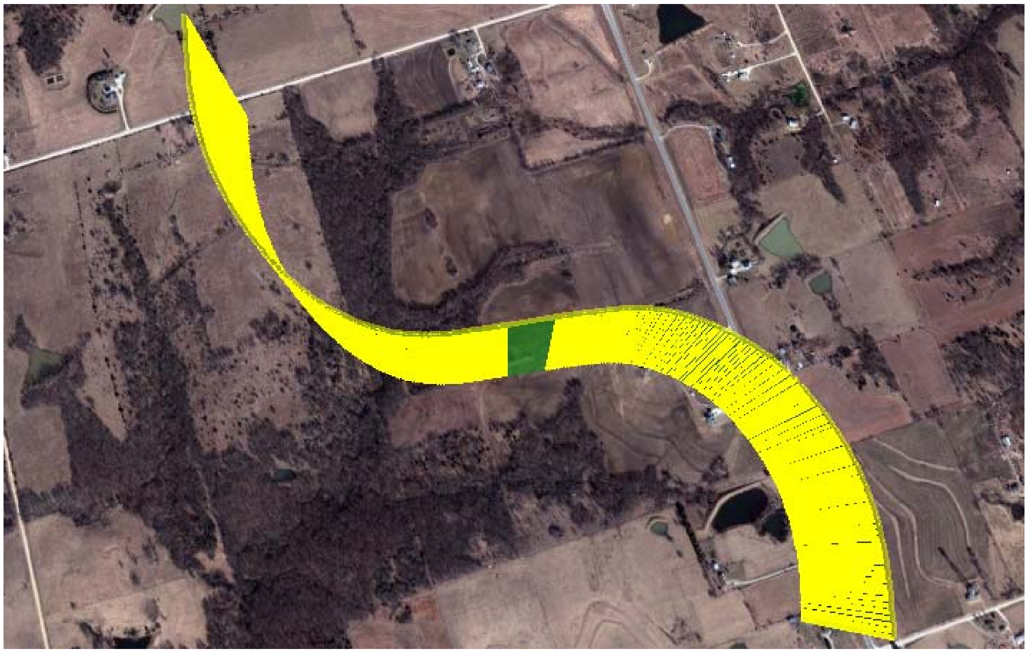


Figure B.22: Slow Flight Turn (Left and Right)

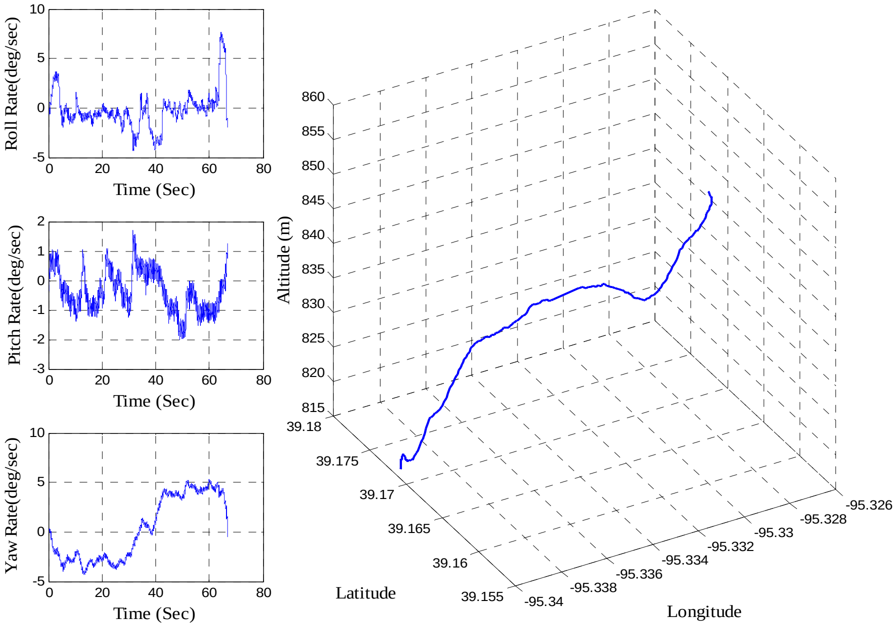


Figure B.23: Slow Flight Turn

Figures B.24 and B.25 show the aircraft in slow flight with varying flap settings. The maneuver was conducted with 10, 20, 30, and 40 degrees of flap. The data was recorded in a single file for the entire maneuver. The gap shown in Figure B. 24 was due to the pause between the different flap settings. No packet losses were observed during this maneuver.

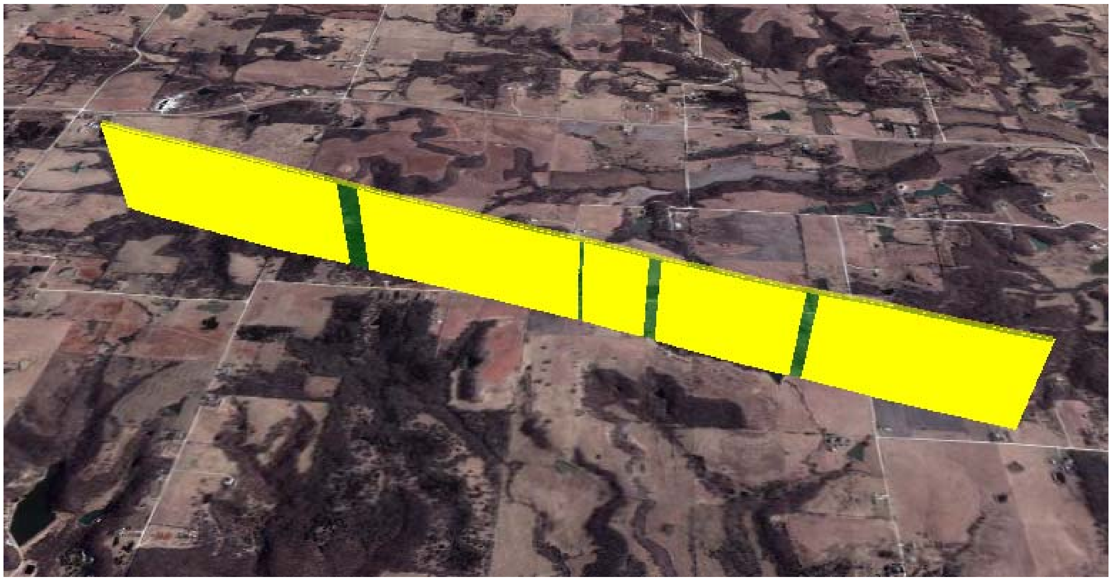


Figure B.24: Google Earth Screenshot of the Slow Flight with Varying Flap Settings

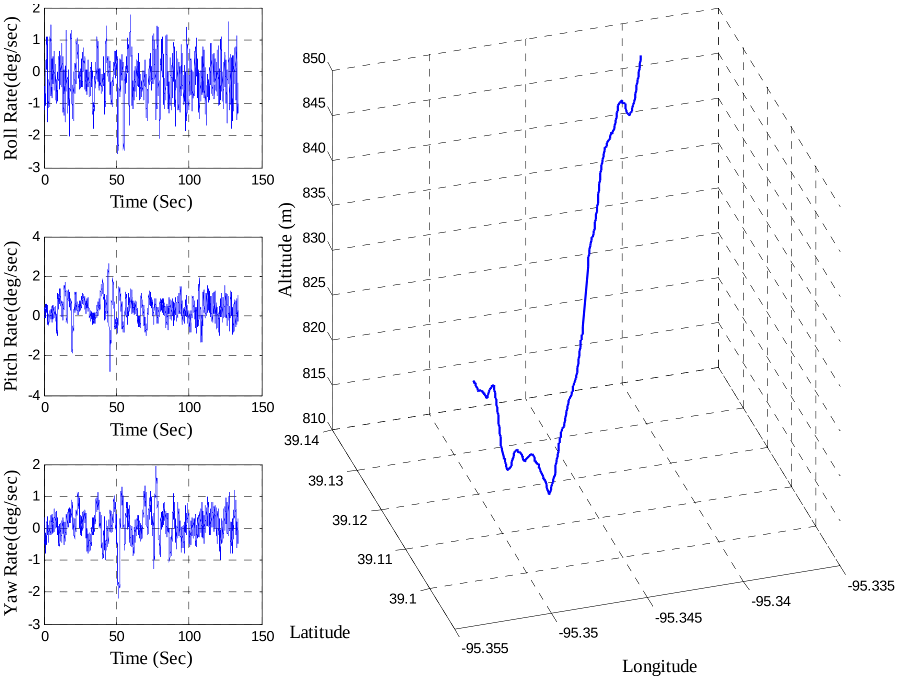


Figure B.25: Slow Flight with Varying Flap Settings

Figures B.26 and B.27 show the accelerated flight documented using Google Earth and MATLAB, respectively. The trim flight condition was accelerated from 75 mph IAS to 110 mph IAS over 25 seconds. No packet losses were observed during this maneuver.

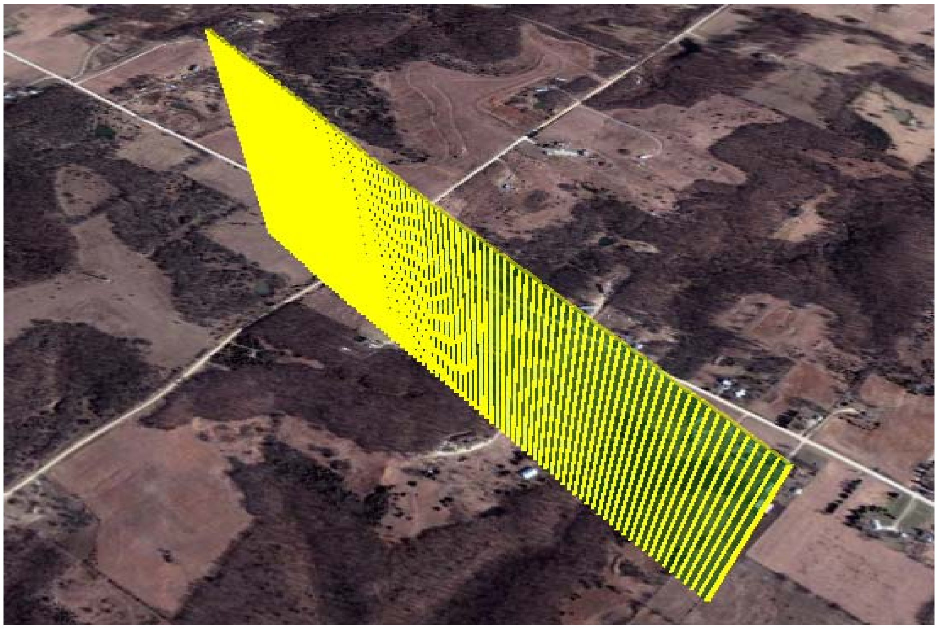


Figure B.26: Google Earth Screenshot of the Accelerated Flight with Varying Flap Settings

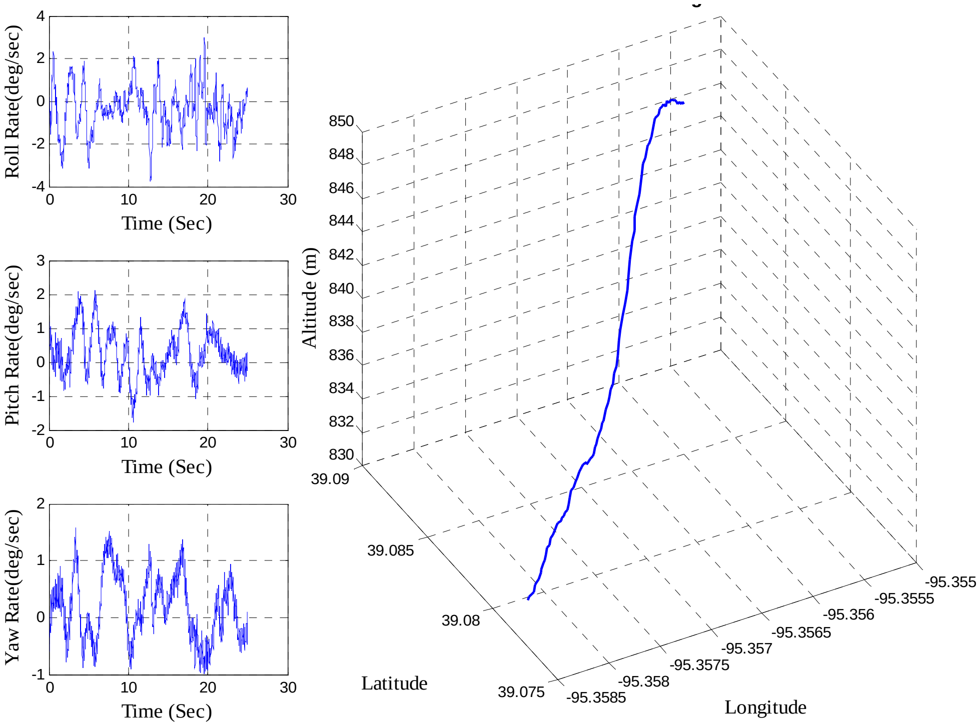


Figure B.27: Accelerated Flight

Figures B.28 to B.33 show the flight track and the MATLAB plots during frequency sweep maneuvers using elevator, rudder and aileron. Control surface commands were given for an increasing frequency sine wave, known as a chirp or a frequency sweep, starting at approximately 1 cycle every 5 seconds to 2 cycles in 1 second. No losses were found during the elevator and aileron frequency sweeps. Packet losses were observed during the rudder frequency sweeps.

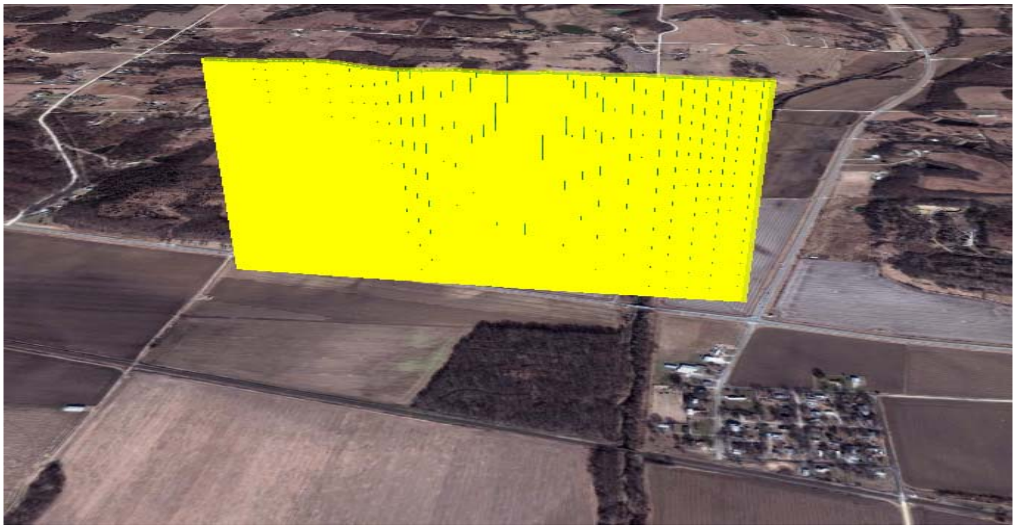


Figure B.28: Google Earth Screenshot of the Frequency Sweep of the Elevator

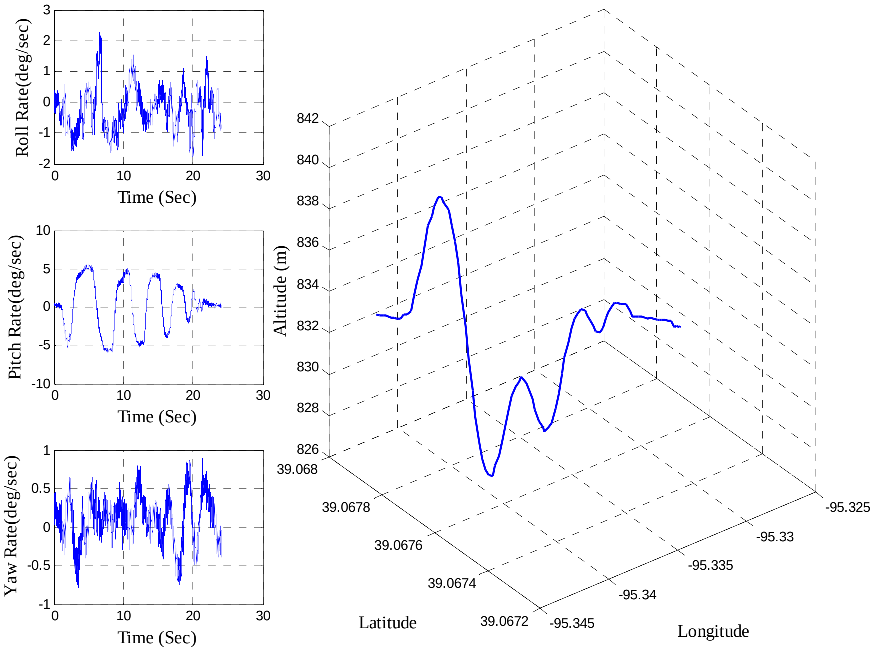


Figure B.29: Frequency Sweeps of the Elevator

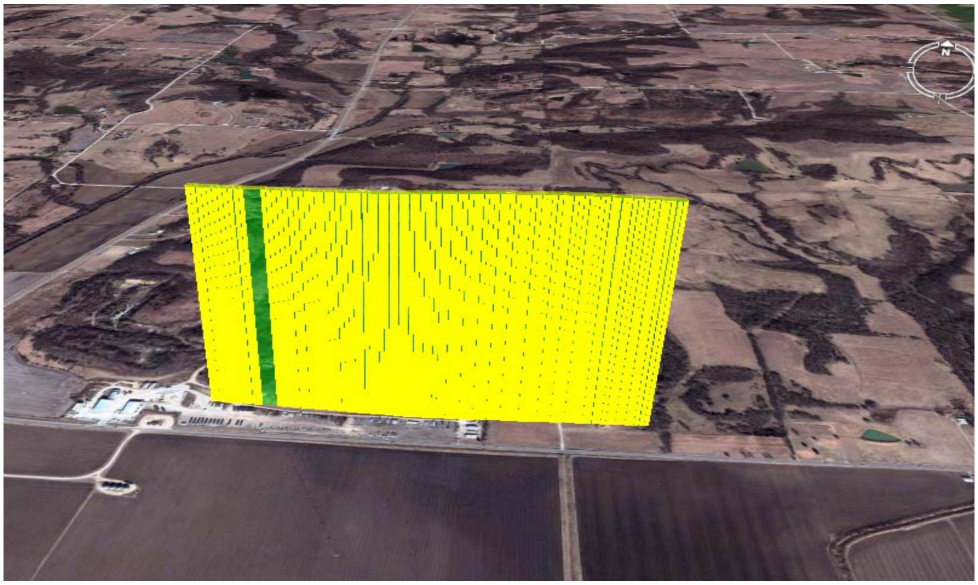


Figure B.30: Google Earth Screenshot of the Frequency Sweeps of the Rudder

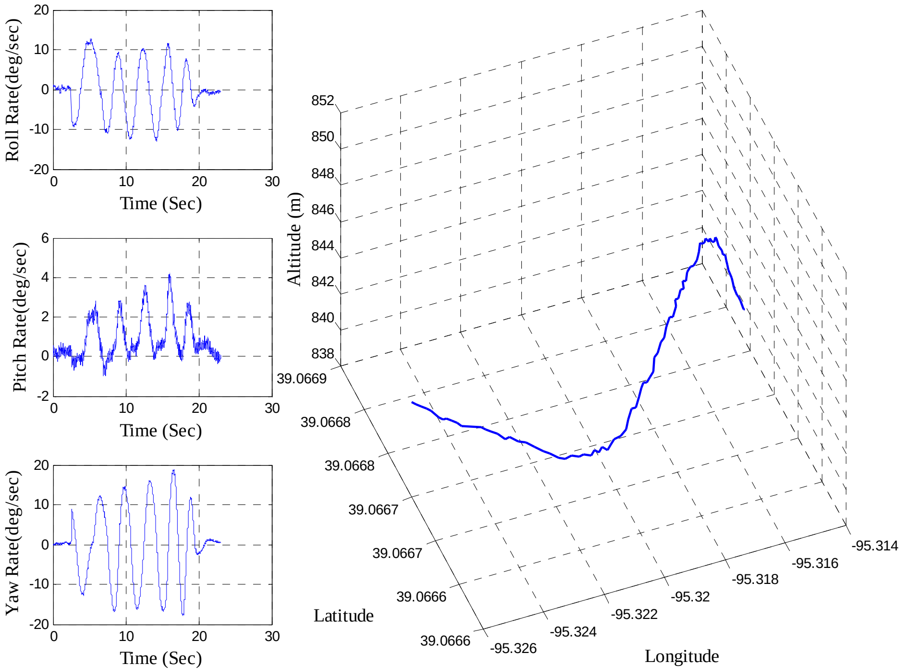


Figure B.31: Frequency Sweeps of the Rudder

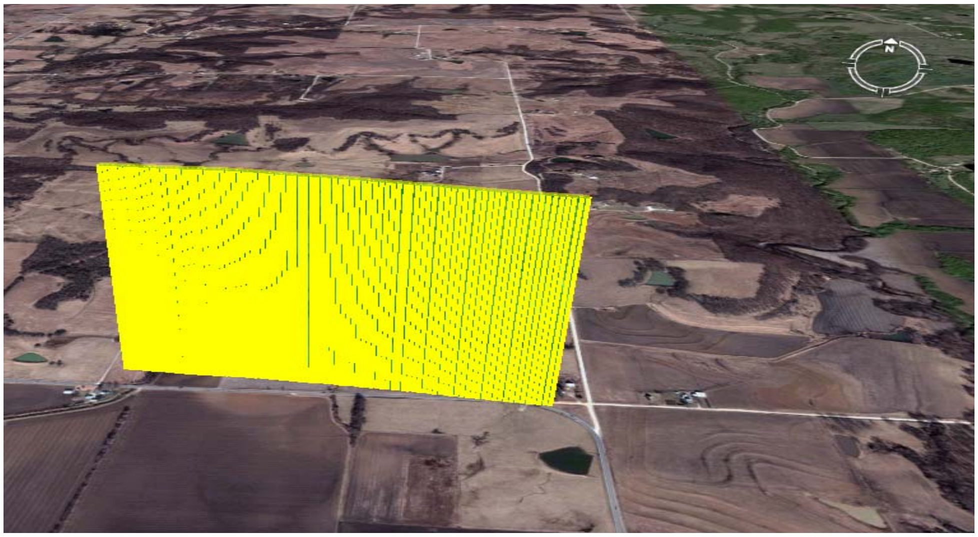


Figure B.32: Google Earth Screenshot of the Frequency Sweeps of the Aileron

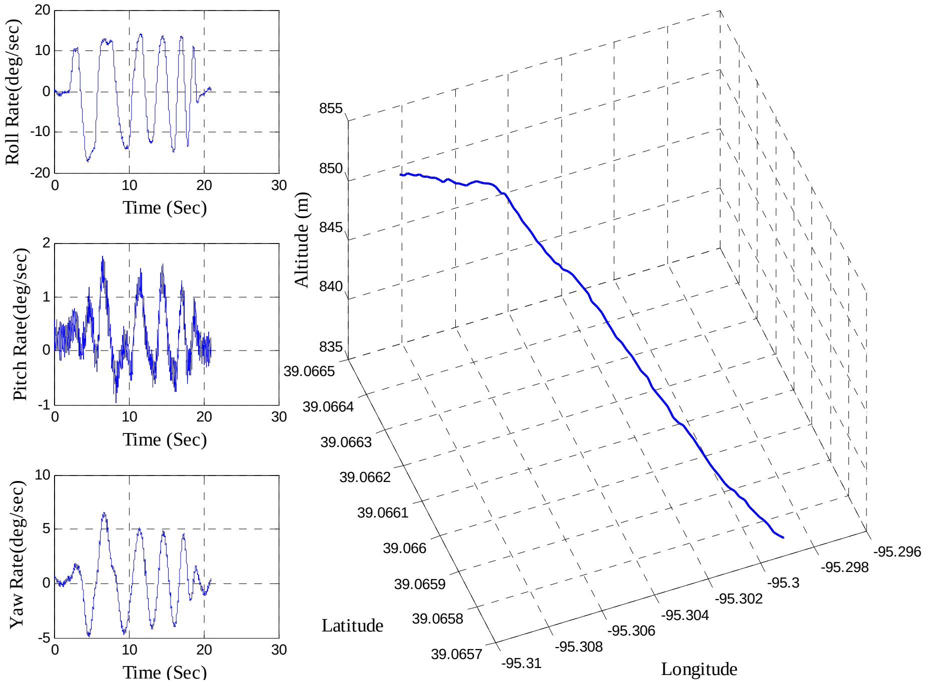


Figure B.33: Frequency Sweeps of the Aileron