Investigate the Development of a Wireless Flight Test System

By

Pradeep Attalury

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

Date Defended 12/02/2009

The Thesis Committee for Pradeep Attalury certifies that

this is the approved version of the following thesis:

Investigate the Development of a Wireless Flight Test System

Chairperson ______________________________
Dr. Richard Colgren

Committee Members ______________________________
Dr. David Downing

____
Dr. Mark Ewing

Date Approved 12/15/2009

Abstract

This thesis describes the development and fight testing of a wireless flight test data acquisition system based on the IEEE 802.11 a/b/g protocols using low cost Commercial-Off-The-Shelf (COTS) equipment and software. The tested system consists of a video node, an Attitude Heading Reference System (AHRS), an Access Point and a User Interface Node. The video node consists of an IP Camera which was used to demonstrate the viability of including video recording as a service in an aircraft. The Attitude Heading Reference System was integrated with a GPS and a serial device server. The User Interface Node was installed with moving map software which receives the data from the AHRS and GPS to display flight information including topographic maps, attitude, heading, and velocity and roll/pitch/yaw rates. It was also used to record data from the video node. The Access Point was used to configure the network in the “Infrastructure mode”. The system was also tested in the “Ad-Hoc mode” i.e., without an Access Point and suggestions for improving the performance of a system in the Ad-Hoc mode were made. The Infrastructure mode was flight tested in a Cessna 172. The data logged from the wireless AHRS during the flight test shows that it performed at its rated specification and that no data was lost due to disconnection in the wireless system. The post flight test data processing shows that the wireless system provided a secure, interference free connection with a throughput of 1.102 Mbps. By comparison, the popular ARINC 429 data bus supports a data rate of 100 Kbps. The developed system demonstrates the applicability of wireless networking using the IEEE 802.11 protocols for application in flight testing and based on this, future work like extending the system to include more number of clients is presented.

Acknowledgements

I would like to thank and express my sincere gratitude to Dr. Richard Colgren, who had been very supportive throughout my endeavor at the university. I would also like to thank Dr. David Downing and Dr. Mark Ewing for agreeing to be a part of the thesis committee, reviewing the report and helping me improve it with their perspective. I would also like acknowledge the Aircraft Design Manufacturing Research Center (ADMRC) at Wichita for funding the research endeavor.

My special thanks to Amy Borton for helping me with the procedures of the department, Andy Prichard, Wesley Ellison and pilot Ron Renz for their support and help during the various stages of my work, especially during flight testing.

I would like to thank my friend Satish for his support and advice throughout my stay at the university and especially for helping me with my research.

Table of Contents

List of Figures

List of Tables

1. Introduction

Developments and breakthroughs in the field of wireless communication and protocols, such as the IEEE 802.11a/b/g, with new modulation schemes have made high data rates possible. The demand for using these new technologies for computer networking and communication in the aviation industry has been growing steadily because of their low cost, decreased weight, ease of operation and enhanced performance. The bandwidth of IEEE 802.11a/b/g wireless protocols is sufficient to support data applications for avionics systems.

1.1. Problem Statement

This section presents the characteristics of the existing avionics data buses to illustrate the need for more efficient means of data transfer. The applicability of the IEEE 802.11a/b/g protocols in avionics is also presented.

Commercial avionics systems have always employed point-to-point connections between each system including air data computers, navigation systems, engine control systems and digital electronics. ARINC 429 is the most commonly used data bus for commercial and transport aircraft. Messages are transmitted at a bit rate of either 12.5 kilobits per second or 100 kilobits per second over wires in twisted pairs. Two buses are used for bi-directional communication between the systems. Military avionics use the MIL-STD-1553 multiplex data bus because of its advantages in weight reduction and simplicity. It is a bi-directional data bus and supports data rates of up to 1 Mbps. ARINC 629 is a new standard for use in avionics systems and it supports data rates of up to 2 Mbps. It is a relatively expensive and heavy implementation due to the need for custom hardware. Always advancing computing and digital avionics instrumentation creates a need for protocols with enhanced data rates for interconnecting the subsystems without adding to the cost and weight.

The modern technologies in avionics systems are very data intensive. They are being developed with the objectives of making aviation even safer, aiding air traffic management and improving serviceability and maintainability of the systems. Systems like ADS-B (Automatic Dependent Surveillance – Broadcast), FIS-B (Flight Information Services – Broadcast) require data rates in excess of 1 Mbps. They provide information on weather, air traffic and Temporary Flight Restrictions (TFRs) in real time, to the pilot, on the Cockpit Display Unit (CDU). Various systems are being designed with intelligence to help predict and identify a part or system that needs maintenance or replacement. Such systems need to be interconnected with the onboard instrumentation to meet the objective. The protocols and standards in use are not designed for such data intensive systems involving complex networking. Implementing a wireless network, based on the IEEE 802.11a/b/g protocols, is a viable alternative with many advantages. The network will prove cost effective because expensive cables are not required, the weight reduction from eliminating the cables will be considerable. These protocols also support data rates of up to 54 Mbps. The high data transmission rate of these protocols implies they can be used for data intensive applications like video, voice and data transfer over the same network.

1.2. Previous Work

At this point, it is important to mention that the research presented in this thesis is a continuation and an extension of the research work done by Mr. Satish Chilakala at the University of Kansas. His work characterizing the individual IEEE 802.11a/b/g protocols for application in the development of an avionics system is the basis for the research presented in this report. In characterizing the protocols, network testing tools were identified, the range and operation of the protocols was tested and a two node network of a laptop computer and a wireless Attitude Heading Reference System (AHRS) was tested in the Ad-Hoc mode [1].

Continuing work on the topic, this thesis presents the development of a wireless flight test system along with the analysis of the data from flight testing the system. Nodes were identified for being included in the wireless flight test system and a test system comprising a wireless Attitude Heading Reference System, an IP Camera, an Access Point and a User Interface Node has been developed and flight tested.

Wireless technology is being considered for various applications in the aviation industry because the reliance on point-to-point connected systems, with conventional cables and connectors, is proving to be very disadvantageous for aircraft operators. Such systems add a lot of weight to the aircraft. Troubleshooting and fault identification in such systems is a cumbersome and time consuming process and upgrading and replacing an existing avionics system is an even more difficult task. These shortcomings of a wired network can be overcome by implementing a wireless network. It would offer flexibility and ease of operation and maintenance. The aviation industry's need for innovative alternate means of data transfer which supports data intensive applications without the hassles of a wired installation has spurred considerable research and development. Many commercial products and systems are now available for use on an aircraft, which use wireless connectivity instead of cables. This section describes the research and developments of wireless avionics systems in the aviation field.

A structural health monitoring system based on the Bluetooth wireless standard was tested by the Lockheed Martin Aeronautics Company. The system was comprised of many sensors connected wirelessly by Bluetooth connections and were distributed along the airframe of an F-16B test aircraft. It was developed for prognostic health monitoring. Bluetooth or the IEEE 802.15.1 protocol is an industry standard for Personal Area Network (PAN). It supports data rate of up to 3 Mbps in Version 2.1 and up to 24 Mbps in Version 3.0. It has a range of 10 to 100 meters based on the class of the device [2].

Honeywell has developed FliteLink based on Wireless Fidelity (Wi-Fi) and General Packet Radio Service (GPRS), for its Flight Data Acquisition and Management System (FDAMS). It provides fast, efficient and timely data for the airline’s flight operation, unlike the conventional way of collecting data on magnetic memory storage cards. FliteLink, shown in Figure 1.1, automatically downloads flight and aircraft data, providing fast, efficient, and timely information to airline Flight Operations. Using 802.11 (Wi-Fi) and cellular/GPRS networks, FliteLink provides immediate access to flight data, thereby accelerating Flight Operational Quality Assurance (FOQA) decision making. At the same time, FliteLink lowers data retrieval operating costs when compared to the Aircraft Communications Addressing and Reporting System (ACARS) transmissions or the logistics of manual data retrieval. Larger data packages can be downloaded faster, more frequently, and more reliably than by direct downloading from the FDAMS or by collection of magnetic memory storage cards [3].

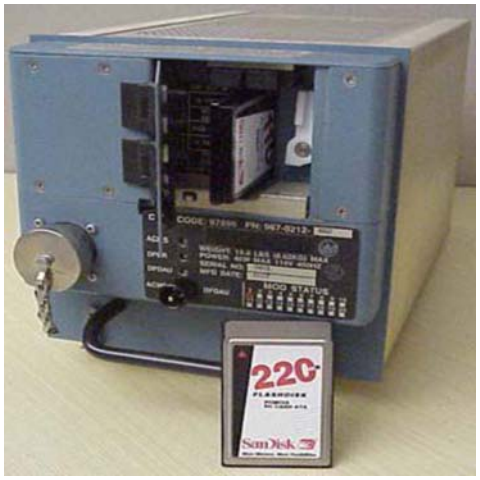


Figure 1.1: FliteLink System of Honeywell

The Wireless Smoke Detection System, developed by Securapalne Technologies LLC, was one of the earliest wireless point-to-point intra-aircraft transmission systems to get certified for use on a commercial airplane. Figure 1.2 shows the architecture of the system. More than 1000 airplanes are deployed with this system. Airlines and other installers have experienced approximately 50 percent fewer installation man-hours for the Securaplane system versus a wired system [4].

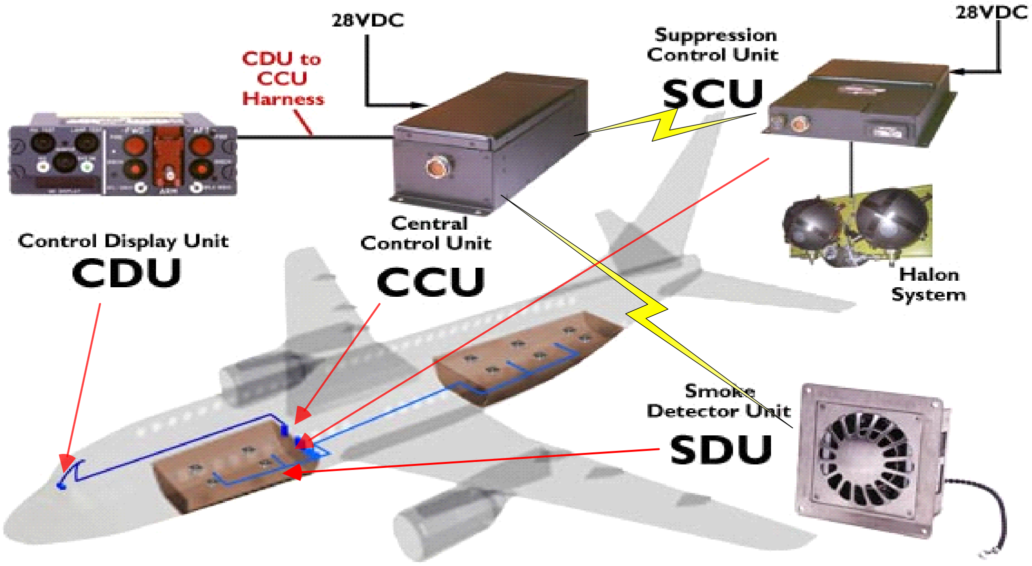


Figure 1.2: The Wireless Smoke Detection System by Securaplane Technologies

Another system, the SkyFi™ 2000 of IMS Flight Deck, shown in Figure 1.3, is designed to deliver satellite weather and GPS information to a Class 1 or Class 2 Electronic Flight Bag (EFB) simultaneously without wires. It converts the signal from a satellite weather or GPS receiver to a standard 802.11 wireless signal that can be accessed by any EFB equipped with a wireless adapter [5].

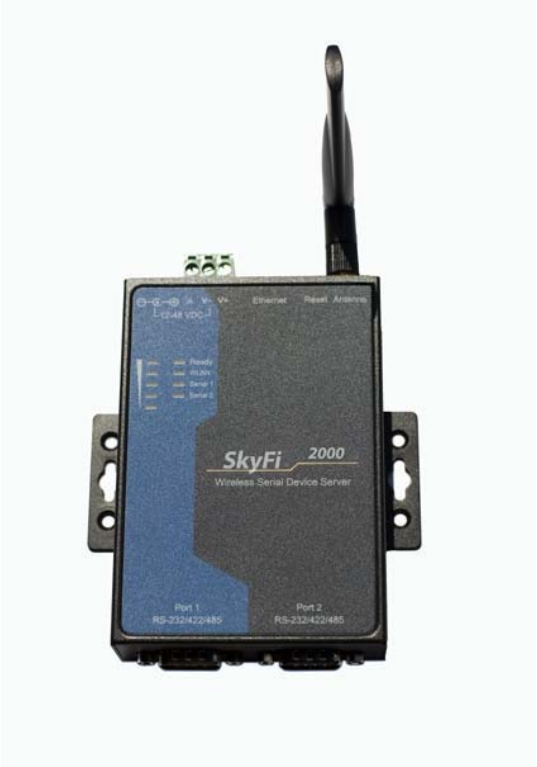


Figure 1.3: SkyFi 2000 of IMS Flight Deck

On the Boeing 787 Dreamliner, the aircraft crew's secure wireless local area network could be used in conjunction with a wireless Local Area Network (LAN) infrastructure in airline terminals to wirelessly upload flight plan information, cabin inventories and passenger information, without having to take information physically to the airplane. This is an 802.11 system with an extended range of about

300 to 400 feet (91.5 to 122 m), so the airplane doesn't have to be docked and it can still make a connection [6].

Teledyne Controls' Aircraft Local Area Network system (AirLAN) provides operators with a compact, lightweight and cost-effective LAN connectivity solution both onboard the aircraft, and between the aircraft and the corporate network. This integrated system delivers in one single unit the entire infrastructure required for secure wired and wireless onboard Local Area Networks and ARINC 429 devices.

The AirLAN system, show in Figure 1.4, offers additional options such as: ARINC 429 interconnectivity, 802.11 for Terminal Wireless LAN Unit (TWLU) functionality, and/or 802.11 for Cabin Wireless LAN (CWLU) functionality. Teledyne's AirLAN system allows data to be passed from equipment on the ground to equipment onboard the aircraft, and vice versa. As a wireless LAN unit, not only does the AirLAN system eliminate a large portion of the installation cost of wiring the aircraft for Ethernet, but it also allows flexible wireless high-speed access to the airborne LAN from anywhere on the aircraft. With the 802.11 capability added, the AirLAN also provides the capability to move a vast amount of digital data on and off the aircraft [7].

SecureLINK of Avionica Inc. enables secure, wireless transfer of data to and from the aircraft, eliminating the cost and delay of traditional aircraft media such as paper charts, optical disks, PCMCIA cards, USB keys, etc. It establishes an authenticated and encrypted log-on automatically as the aircraft enters the system's 802.11 wireless network. Within moments, it communicates with the Airside Local Area Network to transmit and receive data (TWLU mode) without human intervention, minimizing both labor and material costs, and eliminating the possibility of misplaced media and lost data [8].

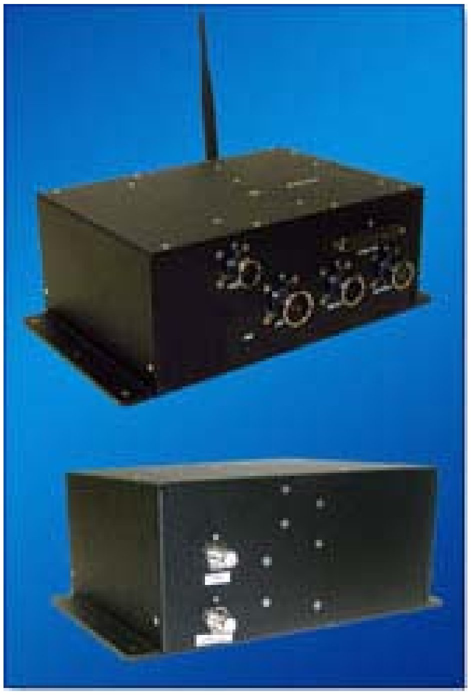


Figure 1.4: AirLAN System of Teledyne Controls

GE Aviation is to develop wireless data gathering and transmission technology for aircraft applications in support of the WiTNESSS (Wireless Technologies for Novel Enhancement of Systems and Structures Serviceability) initiative. Data transfer is essential for many aircraft health monitoring and test instrumentation applications on fixed-wing aircraft, helicopters and engine test beds. The potential advantages of transferring the data wirelessly, for these applications, are many and include: a significant weight saving, simplified integration (as there are no wires/cables to route), and easier access to the data. Conversely, the absence of flight-critical data in these applications makes them an ideal proving ground for wireless technology [9].

Many of these commercially available products are designed as wireless alternatives to an existing system. These products, when installed on an aircraft, are part of a larger wired system. Products like SecureLINK, SkyFi 2000 and AirLan are similar to the nodes that have been incorporated in the wireless flight test system presented in this thesis.

1.3. Approach

The objective of this research endeavor is to investigate and establish the viability of IEEE 802.11a/b/g protocols for flight test application. If proven sufficient, an IEEE 802.11a/b/g protocol based system or subsystem will help reduce the complexity and the associated expenses of installation, operation and maintenance of an equivalent wired system. The current effort involves development of a wireless flight test system, flight testing the system and analyzing the flight test results to prove viability of the application of the IEEE 802.11 protocols for fight testing.

The development of a wireless flight test system required the identification of the nodes to be included in the system. For our system, two types of sensor nodes were identified. The first was a wireless-enabled inertial measurement unit. This node comprised of a NAV 420 and a WiBox® Serial Device Server and is referred to as the Wireless Attitude Heading Reference System (W-AHRS) henceforth. The second node comprised of a wireless-enabled video camera. Along with these sensor nodes, the flight test system also consisted of a wireless Access Point and a laptop computer that was used as the User Interface Node. Figure 1.5 shows the wireless flight test system which was developed and flight tested. The description of individual nodes is given in Chapter 3.

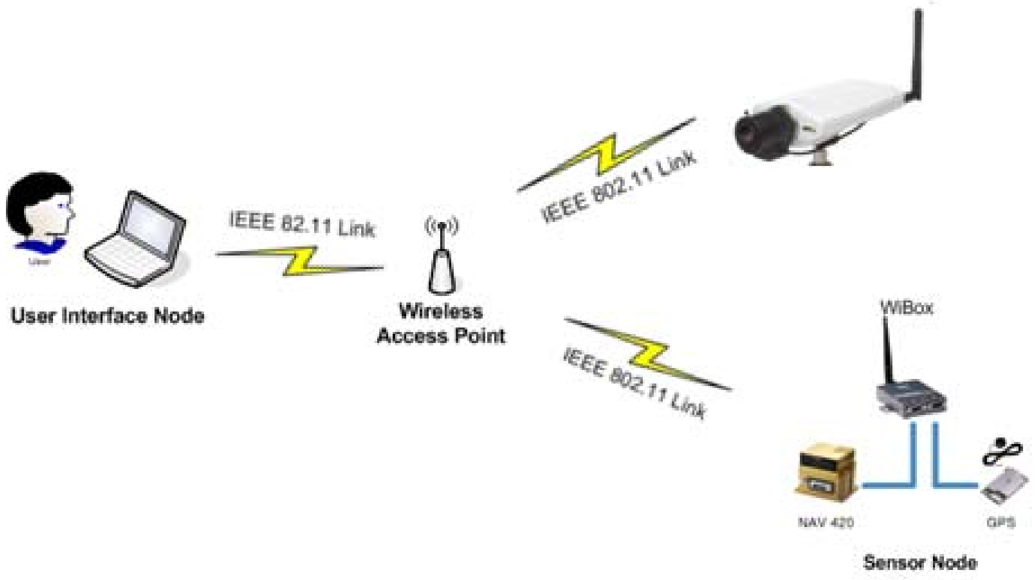


Figure 1.5: Wireless Flight Test System

The developed system consists of sensor nodes that have applicability in flight testing. Similar sensors are employed as part of advanced electronic flight bags on aircrafts. The sensor nodes thus provide useable data for generating the wireless traffic. The developed system was tested for throughput, packet round trip time, continuity and signal to noise ratio of the wireless link, to investigate the viability of the application of the IEEE 802.11 protocols for flight test systems. These parameters of a wireless connection help in evaluating the performance of the wireless network and also enable identification of network congestion, loss of connection, and interference to the wireless communication of the system. The developed system was tested on the ground in two network configurations, namely the Ad-Hoc mode and the Infrastructure mode. The infrastructure mode was then employed for flight testing the system. The description of the Ad-Hoc mode and the Infrastructure mode is given in Chapter 2 and a comparison of the test results is provided in Chapter 6.

2. Background

The IEEE 802.11a/b/g standard encompasses wireless local area network (WLAN) computer communication in the unlicensed 2.4 GHz, 3.6 GHz and 5 GHz frequency bands. This section gives an overview of the protocols, topologies of the wireless local area networks and the IP Addressing system employed in this research.

2.1. IEEE 802.11 Protocols

IEEE 802.11 is a group of specifications developed by the Institute of Electrical and Electronics Engineers Inc. (IEEE) for wireless local area networks (WLANs). These specifications define an over-the-air interface between a wireless client and a base station (or access point), or between two or more wireless clients. The wide spread use of these protocols in home networking and their many industrial applications have seen a continuous development in the IEEE 802.11 standard.

- The 802.11 standard was first ratified in 1997. It specified bit rates of 1 Mbps and 2 Mbps in the 2.4 GHz. It is obsolete today.
- In 1999, the 802.11 standard was ratified to define the 802.11b specification. 802.11b has a maximum raw data rate of 11 Mbps and uses the same media access method defined in the original 802.11 standard.

- At about the same time of defining the 802.11b protocol, the IEEE also defined the 802.11a standard. 802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks.
- In June 2003, the 802.11g standard was ratified. This standard built on the features of the previous two protocols. It operates in the 2.4 GHz frequency and supports up to 54 Mbps.

There has been a continuous development in the IEEE 802.11 standard to address issues as network security, include advanced encryption standards, and to enhance the supported bandwidth to more than the present 54 Mbps. These are being developed under various IEEE groups. Some of these groups and their areas of work are given below:

- 802.11 - The original WLAN Standard which supported 1 Mbps to 2 Mbps.
- 802.11a - High speed WLAN standard for 5 GHz band. It supports data rates of up to 54 Mbps.
- 802.11b - WLAN standard for 2.4 GHz band. It supports data rates of 11 Mbps.
- 802.11d – It adds support for international roaming, enabling configuration of devices to meet local RF regulations.

- 802.11e - Addresses quality of service requirements for all IEEE WLAN radio interfaces.
- 802.11f - Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
- 802.11g - Establishes an additional modulation technique for 2.4 GHz band. Supports speeds up to 54 Mbps. 802.11h Defines the spectrum management of the 5 GHz band.
- 802.11k - Defines and exposes radio and network information to facilitate radio resource management of a mobile Wireless LAN.
- 802.11n - Provides higher throughput improvements. Intended to provide speeds up to 500 Mbps.
- 802.11s - Defines how wireless devices can interconnect to create an Ad-Hoc (mesh) network.
- 802.11r - Provides fast (<50 millisecond), secure and QoS-enabled inter-access point roaming protocol for clients.
- 802.11u - Adds features to improve interworking with external (non-802) networks where the user is not pre-authorized for access.
- 802.11v - Enhances client manageability, infrastructure assisted roaming management, and filtering services.
- 802.11z - Creates tunnel direct link setup between clients to improve peer-peer video throughput.
- 802.11aa - Robust video transport streaming.

The features of the 802.11 a/b/g protocols are summarized in Table 1.

Standard	**Modulation Scheme**	**Frequency Band**	**Data Rate**	**Advantages**	**Disadvantages**
802.11a	OFDM	5 GHz UNII band	6, 9, 12, 54, 36, 48 and 54 Mbps	High speed protocol in a band with less interference	Limited range, expensive
802.11b	DSSS or FHSS	2.4 GHz ISM band	1,2 5.5 and 11 Mbps	Cost effective for extended range	Low speed protocol operating in a crowded band
802.11g	OFDM or DSSS	2.4 GHz ISM band	6, 9, 12, 54, 36, 48 and 54 Mbps	High speed protocol compatible with 802.11b	Operates in a crowded band
802.11n	OFDM	2.4 GHz, 5 GHz (concurrent or selectable)	Up to 600 Mbps	Data rates more than 54 Mbps	-

Table 1: IEEE 802.11a/b/g/n Protocols

2.2. Wireless LAN Topologies

Three Local Area Network (LAN) topologies can be employed using the IEEE 802.11 a/b/g protocols. These are:

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

These three network topologies are described in the following sections.

2.2.1. Independent Basic Service Set (IBSS)

The Independent Basic Service Set (IBSS) or Ad-Hoc mode (also called peer-to-peer mode) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network or a central relay system. Figure 2.1 shows an Ad-Hoc network in which all the stations/computers can communicate with each other. For this mode of wireless communication, all the stations/computers must be configured to the same Service Set Identifier (SSID) and channel number. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services. The disadvantage of this network topology is that when there is an increase in the number of stations the channel tends to get crowded, affecting performance.

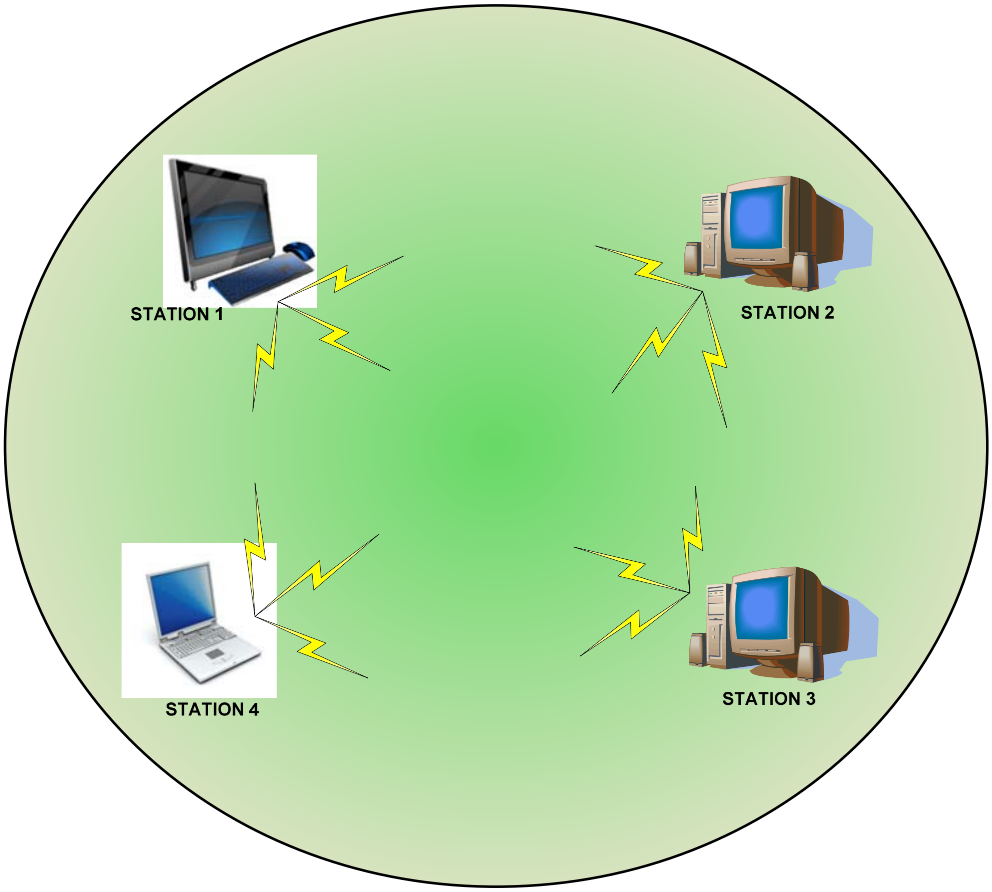


Figure 2.1: IBSS Network Topology

2.2.2. Basic Service Set (BSS)

In the Basic Service Set (BSS) topology, an Access Point (AP) is included in the network to channelize the network traffic. Each BSS is identified by a Service Set Identifier which is a code attached to all packets on a wireless network to identify each packet as part of that network. Besides identifying each packet, an

SSID also uniquely identifies a group of wireless network devices used in a given "Service Set". In this topology, enhanced data rates are achievable and data protection can be incorporated because each station only communicates with the Access Point. Figure 2.2 shows the Basic Service Set Topology.

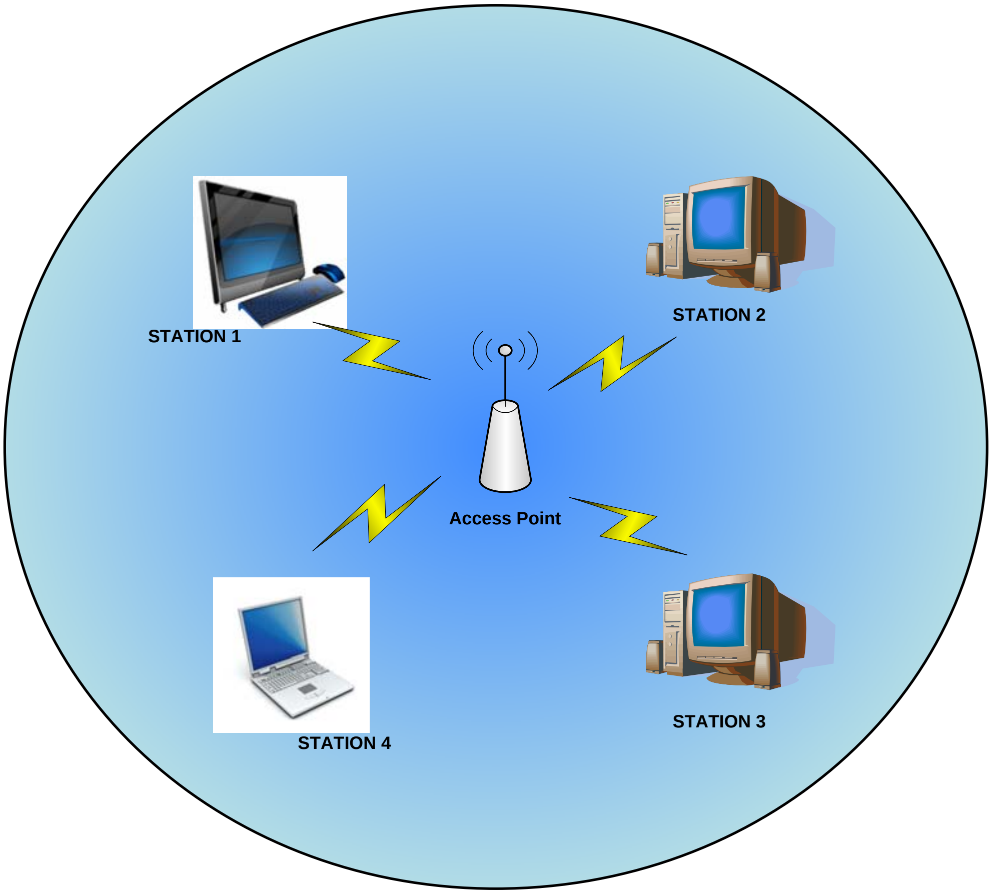


Figure 2.2: Basic Service Set Network Topology

For our research, we have employed the Independent Basic Service Set (IBSS) topology and the Basic Service Set (BSS) topology. Henceforth, the Independent Basic Set topology is referred to as the Ad-Hoc mode and the Basic

Service Set topology is referred to as the Infrastructure mode. The configuration and testing of the nodes in the Ad-Hoc mode and Infrastructure mode are given in Chapters 4 and 5 respectively.

2.3. IP Addresses

The configuration of a wireless network is accomplished by assigning IP Addresses to the components of the network. A brief review of the IP Addressing system and address classes is presented in this section.

IP addresses are 32-bit addresses used by the Internet Protocol to specify source and destination hosts. They simplify readability and are conventionally written in dot-decimal notation which consists of the four octets of the address expressed in decimal and separated by periods. There are 5 classes of IP addresses. These are summarized in Table 2.

Summary of IP Address Classes
Class A - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh • First bit 0; 7 network bits; 24 host bits • Initial byte: 0 - 127 • 126 Class As exist (0 and 127 are reserved) • 16,777,214 hosts on each Class A

Class B - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh • First two bits 10; 14 network bits; 16 host bits • Initial byte: 128 - 191 • 16,384 Class Bs exist • 65,532 hosts on each Class B
Class C - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh • First three bits 110; 21 network bits; 8 host bits • Initial byte: 192 - 223 • 2,097,152 Class Cs exist • 254 hosts on each Class C
Class D - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm • First four bits 1110; 28 multicast address bits • Initial byte: 224 - 247 • Class Ds are multicast addresses
Class E - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr • First four bits 1111; 28 reserved address bits • Initial byte: 248 - 255 • Reserved for experimental use

Table 2: Classification of IP Addresses

In our research, the individual nodes are configured using a Class C IP Address, i.e., IP Address of the form 192.168.XXX with a default subnet mask number of 255.255.255.0. This subnet mask number is a class C default subnet mask number. Our system comprises of only 4 nodes and does not involve sub-networking among them and hence the default subnet mask number was employed.

3. Components of the Wireless Avionics System

In this section, the development of the wireless avionics network system and its individual components are described. Details of the components making the individual nodes are also presented.

To develop a system of wireless nodes that can emulate a basic avionics system, individual nodes of the system were identified. The functionality of each node with regard to an avionics system and with regard to a wireless network was decided upon by taking into account the new commercial off the shelf equipment available. The developed network consisted of the following nodes:

- A Wireless Attitude Heading Reference System
- An Internet Protocol (IP) Camera
- A Flight Data Recorder (FDR)
- An Access Point
- User Interface Node

The schematic of the developed wireless avionics systems and the components of each node of the network are given in Figure 3.1.

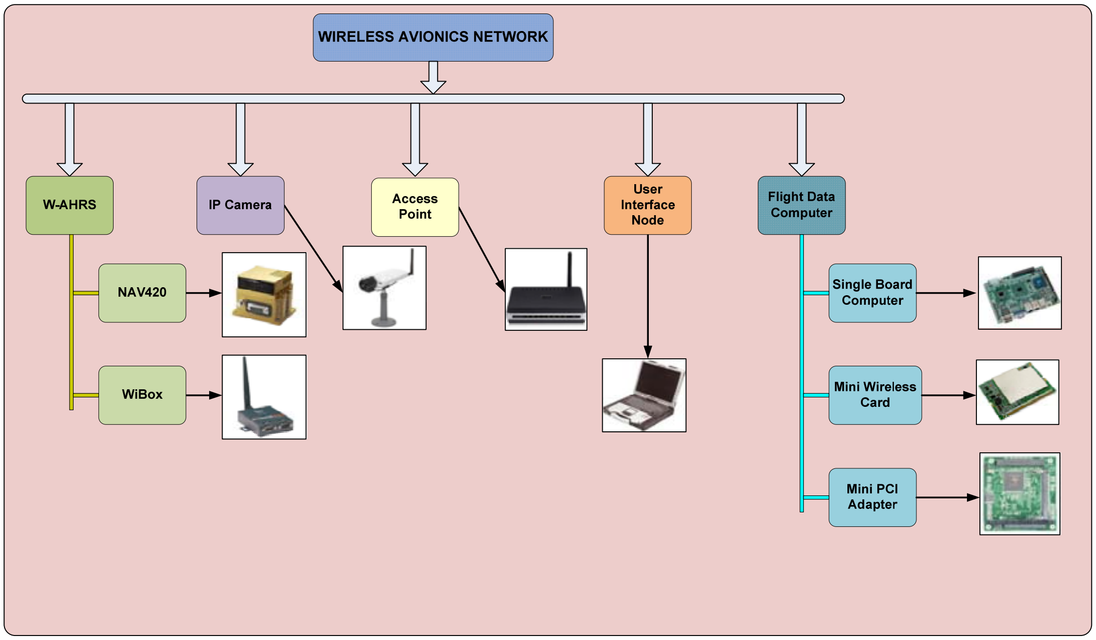


Figure 3.1: Individual Nodes of the Wireless Avionics Network

3.1. Wireless Attitude Heading Reference System

The Wireless Attitude Heading Reference System (W-AHRS) was identified as one of the key sensors to be included in the wireless avionics network. The key criteria for selecting such a sensor were identified as:

- The sensor should measure in-flight data. It should be able to sense and provide data that is pertinent to its application in an avionics environment.

- The data from the sensor should be in a standard format that permits integration of the sensor in to a wireless network, either as a stand alone node in the Ad-Hoc mode or as one of the multiple nodes in the infrastructure mode.

The NAV420 GPS aided Inertial Measurement Unit (IMU) produced by Crossbow® Technologies; connected with a WiBox® Serial Device Server was used in developing the Wireless Attitude Heading Reference System (W-AHRS). The schematic of the W-AHRS is given in Figure 3.2 and the description of the individual components making up the W-AHRS is given in the sections that follow.

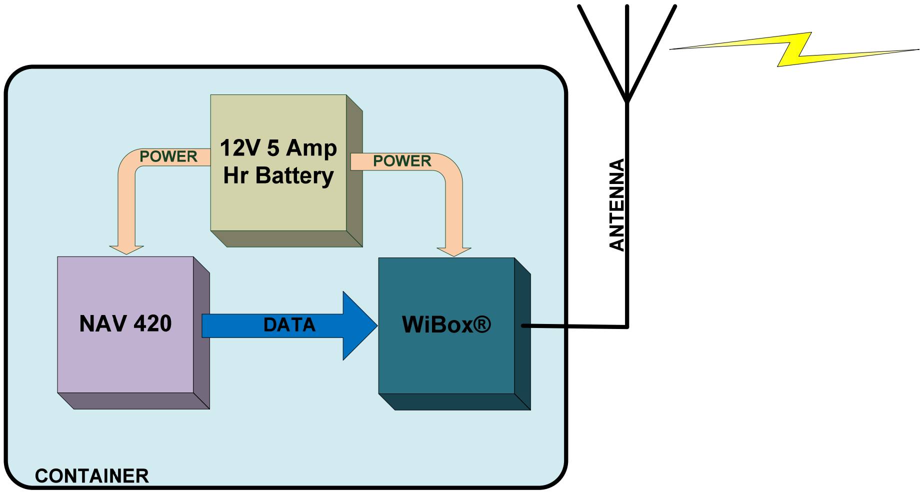


Figure 3.2: Schematic of the Wireless Attitude Reference Heading System

3.1.1. NAV 420

Solid state multi-axis inertial sensors coupled with Global Positioning System (GPS) receivers are an integral part of any modern all glass avionics suite. These sensors are based on Micro-Electro-Mechanical Systems (MEMS). MEMS have revolutionized avionics sensors available, by bringing together silicon-based microelectronics with micromachining technology and making possible the realization of complete systems-on-a-chip. For our sensor node development, we have used the NAV420 produced by Crossbow® Technologies. It is a MEMS based Attitude Heading Reference System. The NAV420 is an advanced and versatile IMU that is less than one-tenth the size and one-tenth the cost of most tactical or navigation grade inertial systems.

The NAV420 from Crossbow Technologies, shown in Figure 3.3, is an attitude heading reference system which incorporates a low cost, solid state Inertial Measurement Unit (IMU). The NAV 420, along with its associated software and a GPS receiver form a GPS-Aided Attitude & Heading Reference system (AHRS) which utilizes both MEMS-based inertial sensors and GPS technology [10].

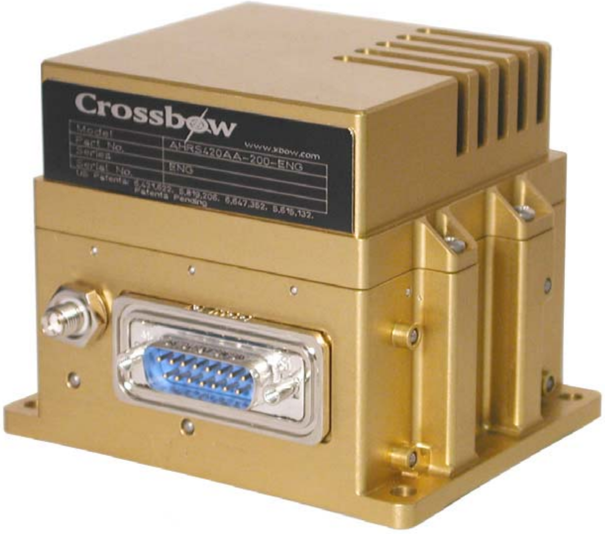


Figure 3.3: NAV420CA – 200

The NAV420 is also a nine-axis measurement system that outputs accurate acceleration, angular rates and magnetic orientation. It consists of the following subsystems:

- Inertial Sensor Array – This is an assembly of three accelerometers, three gyros (rate sensors) and four temperature sensors.

- A three axis fluxgate magnetometer board to compute heading.
- A Wide Area Augmentation System (WAAS) capable GPS receiver for position and velocity measurement.
- A digital signal processing (DSP) module to convert the signals from the inertial sensors and magnetometers into digital data, filter it and computes the attitude solution at 100 Hz output rate.

It has two bi-directional asynchronous serial ports to support user interaction. The user port facilitates the reading of navigation and AHRS output packets through the NAV420's input communication protocol. The NAV420 can be set to output one of the three types of data: a scaled sensor packet of size 34 bytes, an angle packet of size 34 bytes and a NAV packet of size 36 bytes. The user port also supports user configuration and magnetic calibration of the NAV420. National Marine Electronics Association (NMEA) standard GPS messages can also be read from the GPS port.

3.1.2. WiBox Serial Device Server

A serial device server is one that is able to read data from a serial device, using a RS-232 cable, and transmits it to the network. The WiBox serial device server is able to read the data from a serial device, here the NAV420, and is able to transmit the data to the network using the IEEE 802.11b/g protocols. The advantage of the WiBox serial device server is that it enables connection of devices to IEEE 802.11b/g networks and adds wired Ethernet connectivity for more complete configuration and flexibility. The interface software that is provided with the WiBox device eliminates the need for programming on the part of the end user to connect serial devices like the NAV420 IMU to an Ethernet or IEEE 802.11b/g network. The WiBox also addresses network security by incorporating several features as 64/128 bit Wired Equivalent Privacy (WEP), 128 – 256 Bit end to end Rijindael Advanced Encryption Standard (AES) and Wi-Fi Protected Access with Pre Shared Key (WPA-PSK) [11].

The output from the NAV420 is read thorough an RS-232 cable. To transmit this data using a wireless link, a wireless transceiver is required with an ability to read the data from the NAV420 and convert it to a format that is suitable for wireless transmission. The WiBox® Serial Device Server of Lantronix® Inc., shown in Figure 3.4, was selected because it fulfills both these requirements.

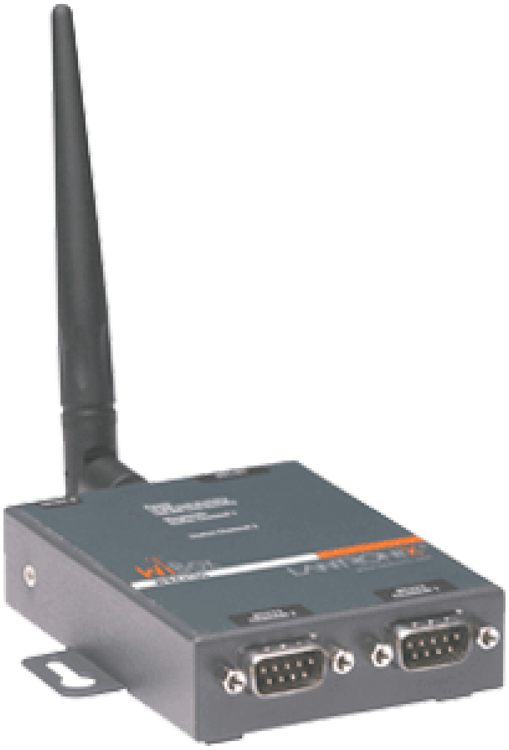
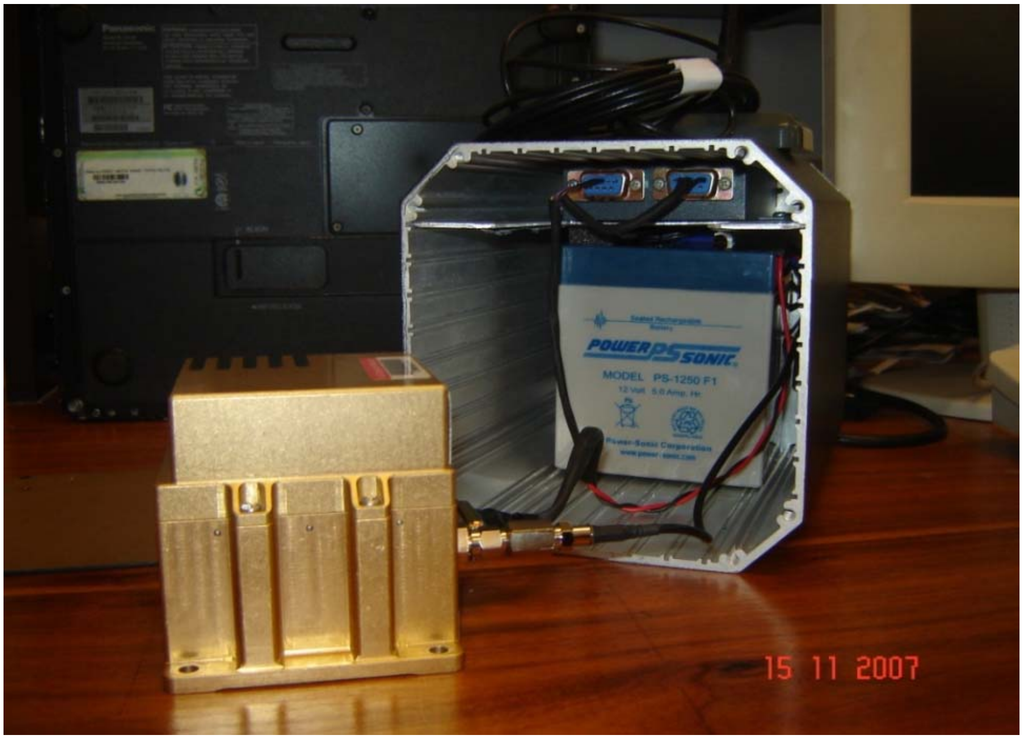


Figure 3.4: WiBox® Serial Device Server

3.1.3. Wireless AHRS Unit

The Wireless AHRS unit was built by integrating the NAV420 with the WiBox serial device server. A GPS antenna was also included to aid the NAV420. The WiBox device server and the NAV420 are powered by a 12V 5Amp Hr lead acid battery. By including a battery, the wireless AHRS unit could operate on a stand alone basis, with no power required from the aircraft during flight testing. The entire module was assembled in a Can-Tainer which is a PC/104 enclosure constructed with 0.125 inch aluminum sheet. It is a rugged enclosure that is designed to withstand the rigors of hostile weather and mobile environments. Figure 3.5 shows the assembly of the Wireless AHRS Unit.



15 11 2007

Figure 3.5: Assembly of the Wireless AHRS Unit

3.2. IP Camera

The next sensor included in the network was a wireless Internet Protocol Video Camera (IP Camera). The IP Camera would enable testing of the wireless network for data intensive applications like video transmission. The IP Camera chosen was the AXIS® 211W model. This model, shown in Figure 3.5, was selected because of its built in wireless capability that made it easy to integrate it into a network and also because it permitted independent evaluation of the IEEE 802.11 protocol in a peer to peer connection [12].

Figure 3.6: AXIS 211W IP Camera

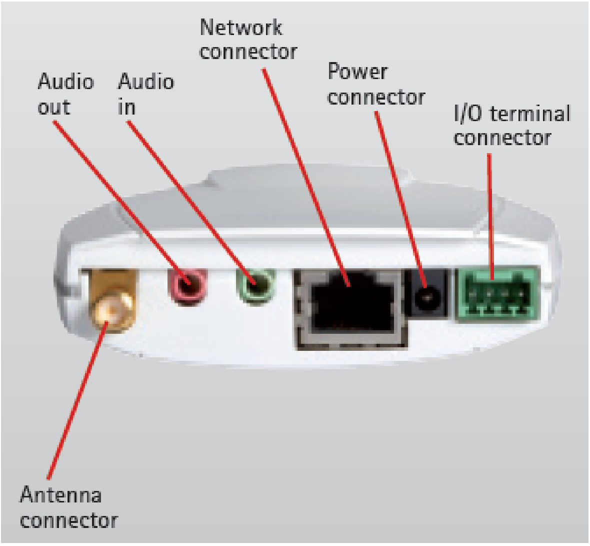


Figure 3.7: AXIS 211W IP Camera, Rear View

The AXIS 211W IP Camera supports the IEEE 802.11b protocol at 1 – 11 Mbps and supports the IEEE 802.11g protocol at 6 – 54 Mbps. The camera provides a video feed at a frame rate of up to 30 frames per second with a VGA resolution of 640x480 to 160x120 pixels. Video is streamed in MPEG-4 and Motion JPEG formats that allows for optimization of both image quality and bandwidth efficiency. The camera can be powered from the wired network or from a power outlet. For security, the camera includes WEP, WPA/WPA2 –PSK, multiple user access levels, IP address filtering and HTTPS encryption. For the initial configuration, the camera is connected to a computer by an Ethernet cable. The camera settings can then be changed by accessing the camera wirelessly, through a web browser. The IP camera does not require specialized software to access the video feed streaming from it. A computer that is connected to the network can access the video feed and record it on its hard drive through a web browser. For flight testing, a 12V 30 Amp Hr battery was included to avoid relying on the aircraft power system. This enabled easy approval of the flight test by the safety board, there was no hassle of extensive wiring from the aircraft system and installation of the equipment on the aircraft was an easy process.

3.3. Flight Data Computer

A Flight Data Computer was developed using an EPIC Standard Single Board Computer (SBC) stacked with a Mesa 4167 dual type III Mini-PCI adapter for

PC/104-PLUS bus and an EnGenius™ EMP 8602 Plus mini PCI adapter. The Flight Data Computer is designed to record data from the Wireless AHRS unit and the IP Camera and store it on the compact flash hard drive. The system was enclosed in an aluminum case with provisions made for various connectors from the single board computer. For flight testing purposes, the system was designed to operate on the power from a 12V 30Amp Hr battery. Figure 3.8 shows the flight data recorder that was built.

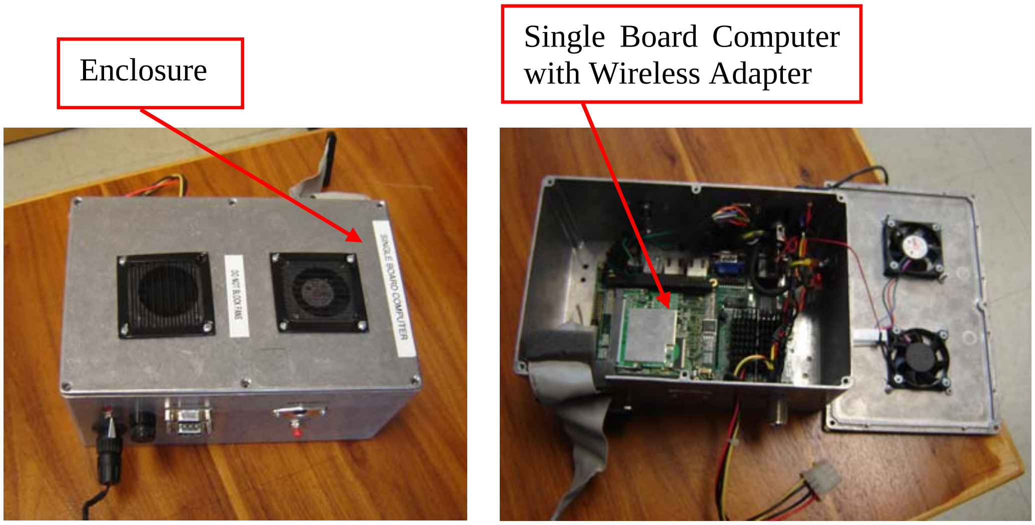


Figure 3.8: Flight Data Computer (2 Views)

3.3.1. Single Board Computer

The Flight Data Computer consists of a single board computer with a compact flash card for storage device. The ReadyBoard™ 800 Embedded Platform for Industrial Computing (EPIC) Single Board Computer (SBC) was selected for building the flight data recorder. The ReadyBoard 800 features a 1 GHz ULV Celeron® M central processing unit with 512 Megabits of Random Access Memory (RAM). It has two 1 Gigabit Ethernet connectors, two USB 2.0 connectors, 2 Serial Comport connectors with onboard compact flash socket. An 8 GB compact flash card is inserted in the compact flash socket. This card is the storage device/hard disc for the computer. Windows® XP operating system is loaded on to this flash card while configuring the computer. A keyboard and mouse are connected to the single board computer using a Y PS/2 cable. Figure 3.9 shows the ReadyBoard 800 EPCI SBC. [13]

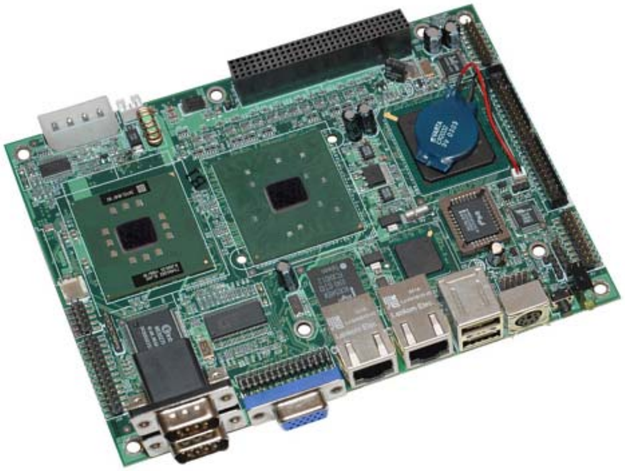


Figure 3.9: Single Board Computer used in Flight Data Computer

3.3.2. Mini PCI Adapter

A mini PCI adapter is required to connect the wireless card to the single board computer. The Mesa 4I67 was used for this purpose. It allows use of 2 MINI-

PCI type III cards, for example wireless network cards, on a PC/104-PLUS host CPU [14]. The 4I67, shown in Figure 3.10, uses a PCI bridge so that it only occupies a single PC/104 slot. The slot where the wireless card is inserted is also shown in Figure 3.10.

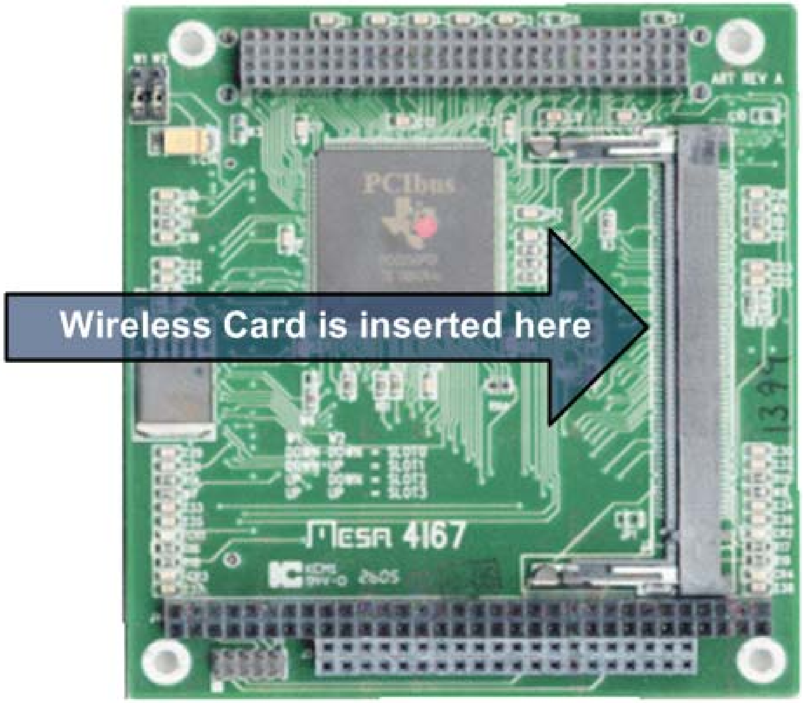


Figure 3.10: 4I67 Mini PCI Adapter

3.3.3. Mini Wireless Card

A mini wireless card was installed to provide wireless connectivity to the single board computer. The EMP 8602 mini wireless card from EnGenius™ Technologies was selected because of its small form factor and its compatibility with the mini PCI Adapter. The EMP 8602 wireless card, shown in Figure 3.11, is also easily configured to operate with the operating system of the single board computer [15].

Figure 3.11: EMP 8602 Mini Wireless Card

3.4. Access Point

A D-Link® WBR 1310 range Booster G Wireless Router was used as an access point. It is a commercial off-the-shelf device used extensively in home networking for providing wireless internet access. This model was chosen as it permitted the router for use in non-internet applications such as our wireless network. It can be configured independently, without the pre-requisite of a DSL or cable internet connection. Figure 3.12 shows the wireless router [16]. For flight testing, the router is run from power from a 12V 30Amp Hr Battery.

Figure 3.12: D-Link® Wireless Router

3.5. User Interface Node

The data from the individual nodes of the network was to be presented to the user to allow for validation and testing of the network. The user interface node was located in the cockpit, during flight testing, for the pilot's reference and duplicated function of a cockpit display unit. During ground tests, it was used to record data and measure network performance by running network analysis tools. A laptop was used as the user interface node for the development and testing of our network of wireless sensors. It was the appropriate choice for the following reasons:

- Network analysis programs that characterize the network performance need to be run from any one of the nodes of the network, as part of the network. A laptop computer with an operating system and wireless card could be included into the network easily. The network analysis programs could also be installed on the computer without requiring extensive independent programming.
- The mobility of the computer was very essential in ground testing of the network. If the user interface node was not mobile, the network could not be tested on the spot. It would have required a fixed arrangement where data would be collected during the test and then the data would have to be processed for evaluation.
- During flight testing of the network, the laptop computer could be used to present the data from the W-AHRS and the IP Camera to the pilot. It could be used as a device to emulate a cockpit display unit, giving the pilot the opportunity to observe in-flight data and performance of the nodes. The laptop computer also obviated the need for extensive wiring to power a display unit during flight tests. It had an inbuilt battery with enough capacity to last for up to 6 hours in between recharges.

The Toughbook CF-29 model, show in Figure 3.13, from Panasonic was used as the user interface node. It is a versatile and rugged computer ideal for use in ground testing and flight testing. It was configured with Windows® XP operating system.

Figure 3.13: User Interface Node

The data from the W-AHRS and the IP Camera was presented to the flight engineer and the pilot by means of interface software that was installed on the laptop computer. The video feed from the IP Camera could be accessed using a web browser like Internet Explorer® or Mozilla Firefox®. The video feed could also be recorded on to the laptop computer through the web browser. The data from the NAV420 of the W-AHRS was presented using the NAV-VIEW software. This software provided the user with attitude and heading information of the aircraft and also permitted data logging from the GPS. To provide the user with the situational awareness, MountainScope™ software from PCAvionics™ was installed on the laptop computer. It uses data from the GPS receiver and provides situational awareness on a moving map which notes high resolution terrain, class B/C/D/E airports, color shaded terrain warning, et cetera. It can also show pitch and roll attitudes of the aircraft using the data from the NAV 420.

4. Ad-Hoc Mode Testing

The development of the complete network based on the IEEE 802.11a/d/g protocols was accomplished in two phases. In Phase I, the two sensor nodes, namely the Wireless Attitude Heading Reference System (W-AHRS) node and the IP Camera were tested independently by configuring them in the Ad-Hoc mode with the laptop computer. In Phase II, the sensor nodes are tested in the Infrastructure mode. The configuring and testing of these nodes in Ad-Hoc mode is described in this chapter. Testing in the Infrastructure mode is described in Chapter 5.

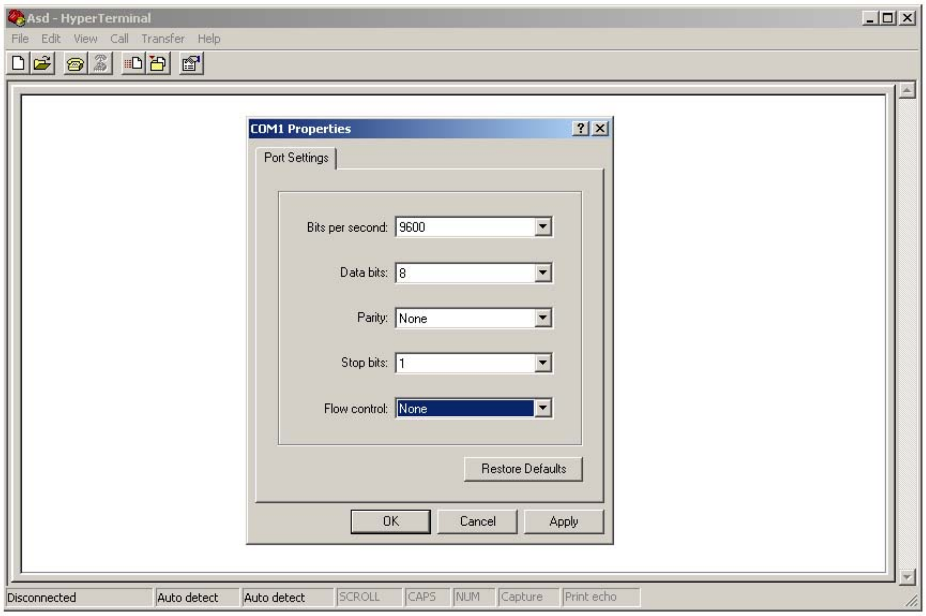
4.1. W-AHRS in Ad-Hoc Mode

4.1.1. Configuring the W-AHRS in Ad-Hoc Mode

The WiBox® Serial Device Server of the W-AHRS was configured to connect with the laptop computer in the Ad-Hoc mode. The WiBox was configured by connecting it to a computer with a DB-9 serial cable. A terminal emulation program, HyperTerminal, was used to access the configuration page of the WiBox serial device server. Figure 4.1 shows the screenshot of the HyperTerminal program along with the settings to access the configuration page of the WiBox serial device server. The connection was made with the settings given in Table 3 and the screenshot of the HyperTerminal window is given in Figure 4.1

COM 1 Properties	
Item	**Setting**
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Table 3: HyperTerminal Settings for WiBox



Bits per second: 9600

Data bits: 8

Parity: None

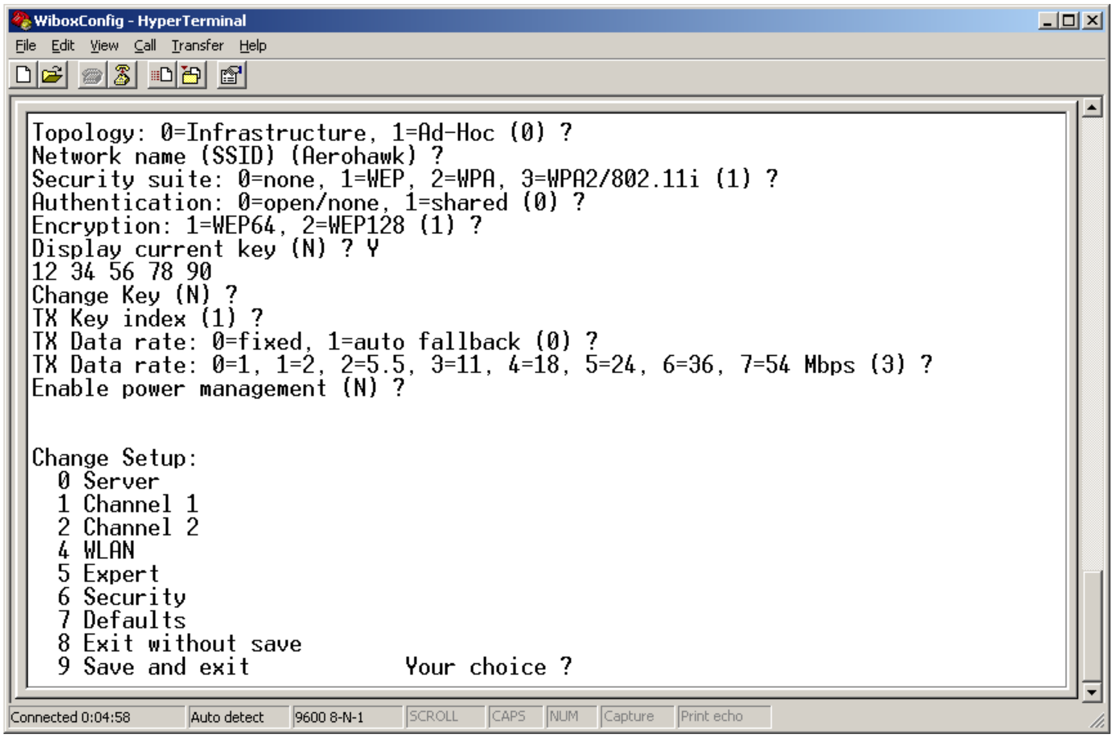
Stop bits: 1

Flow control: None

Disconnected | Auto detect | Auto detect | SCROLL | CAPS | NUM | Capture | Print echo

Figure 4.1: HyperTerminal Settings for WiBox Connection

Figure 4.2 is a screenshot of the configuration page when the WiBox was connected to a computer using a DB-9 serial cable. At the prompt, an option from the displayed menu is selected to configure the WiBox in the Ad-Hoc mode.



```
Topology: 0=Infrastructure, 1=Ad-Hoc (0) ?
Network name (SSID) (Aerohawk) ?
Security suite: 0=none, 1=WEP, 2=WPA, 3=WPA2/802.11i (1) ?
Authentication: 0=open/none, 1=shared (0) ?
Encryption: 1=WEP64, 2=WEP128 (1) ?
Display current key (N) ? Y
12 34 56 78 90
Change Key (N) ?
TX Key index (1) ?
TX Data rate: 0=fixed, 1=auto fallback (0) ?
TX Data rate: 0=1, 1=2, 2=5.5, 3=11, 4=18, 5=24, 6=36, 7=54 Mbps (3) ?
Enable power management (N) ?


Change Setup:
  0 Server
  1 Channel 1
  2 Channel 2
  4 WLAN
  5 Expert
  6 Security
  7 Defaults
  8 Exit without save
  9 Save and exit            Your choice ?
```

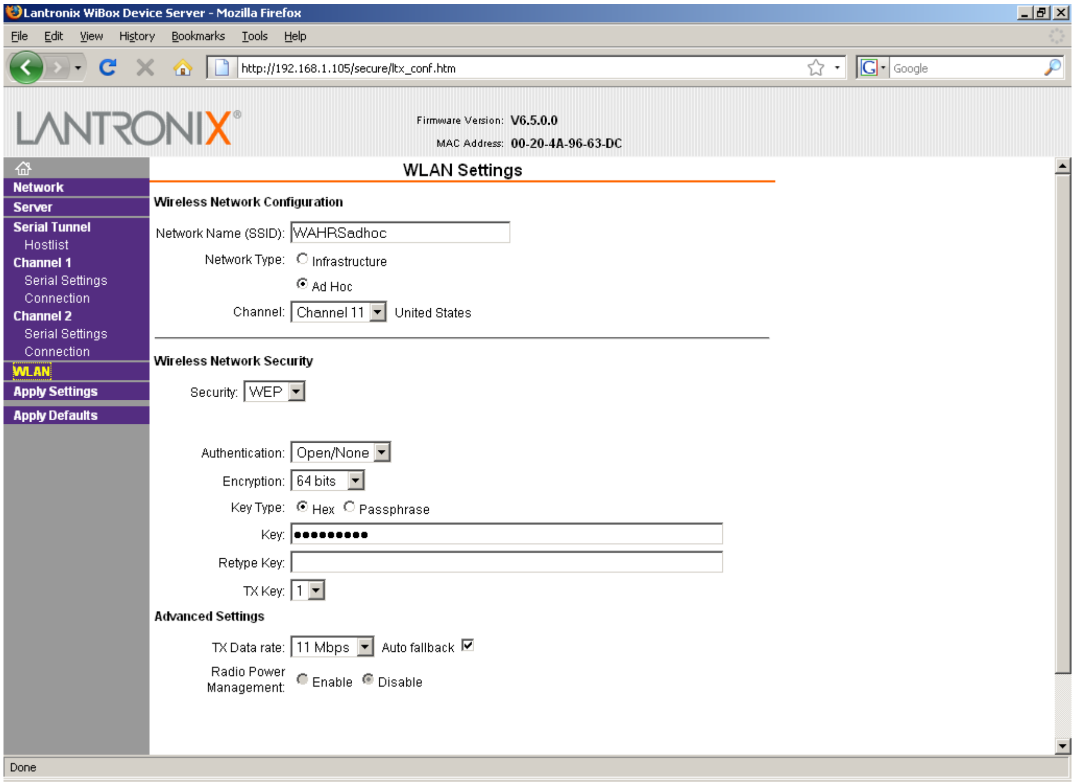
Figure 4.2: Configuration of the WiBox in Ad-Hoc Mode

The WiBox was configured in the Ad-Hoc mode with the settings given in Table 4. With this configuration, the WiBox is set up as a detectable network with the name ‘WAHRSadhoc’ and requires a 10 digit key to establish the connection wirelessly.

Item	**Setting**
Topology	Ad-Hoc
Network Mode	Wireless only
Network Name (SSID)	WAHRSadhoc
IP Address	192.168.1.105
Subnet Mask	255.255.255.0
Default Gateway	None
Security suite	WEP
Authentication	Open/None
Encryption	WEP64
Encryption key	1234567890
TX Data Rate	Fixed
TX Data Rate	11 Mbps
Channel	11

Table 4: Configuration Parameters of the WiBox in Ad-Hoc Mode

After the WiBox was configured to communicate wirelessly, it could be reconfigured without using a DB-5 serial cable. A web browser program can be used to connect with and reconfigure the WiBox from a remote location using the established wireless connection and accessing the configuration page of the WiBox using the IP Address assigned to it. A screenshot of the web browser is given in Figure 4.3, where the various parameters of the WiBox can be configured.



http://192.168.1.105/secure/ltx_conf.htm

Firmware Version: V6.5.0.0
MAC Address: 00-20-4A-96-63-DC

WLAN Settings

Wireless Network Configuration

Network Name (SSID): WAHRSadhoc
Network Type: ○ Infrastructure ● Ad Hoc
Channel: Channel 11 United States

Wireless Network Security

Security: WEP

Authentication: Open/None
Encryption: 64 bits
Key Type: ● Hex ○ Passphrase
Key: ●●●●●●●●●●
Retype Key:
TX Key: 1

Advanced Settings

TX Data rate: 11 Mbps Auto fallback ☑
Radio Power Management: ○ Enable ● Disable

Figure 4.3: Screenshot of the Configuration Page of the WiBox in a Web Browser

The serial port of the WiBox was configured to connect with the NAV 420 and transmit the data wirelessly. The settings for the Serial Port 2 of the WiBox are given in Table 5. The configuration of the serial port on the WiBox completes the configuration of the WiBox serial device server in the Ad-Hoc mode.

Serial Port 2 Settings	
Item	**Setting**
Protocol	RS232
Baud Rate	38400
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None
Pack Control	None
Endpoint Configuration (Local Port)	10001

Table 5: Serial Port Settings for the WiBox

The laptop computer is equipped with a wireless card, which enables connection to a wireless network in the Ad-Hoc mode or in the infrastructure mode. It was configured with the network IP address given in Table 6. The data received from the NAV 420, via the WiBox, is logged using the NAV-VIEW software of Crossbow Technologies.

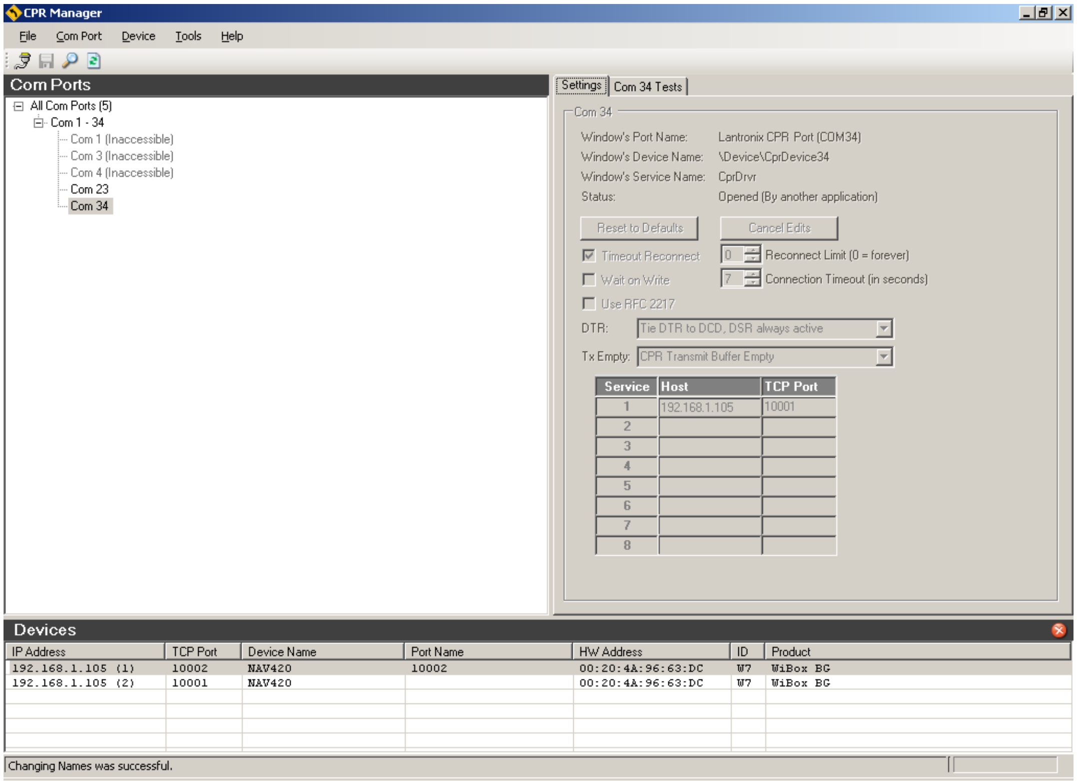
Item	**Setting**
IP Address	192.168.1.105
Subnet Mask	255.255.255.0
Default Gateway	None

Table 6: TCP/IP Settings for the WiBox

The NAV-VIEW software reads data from a serial port. Here, a virtual comport was used to communicate with the NAV420 through the WiBox. A virtual comport was created using the Comport Redirector Software. A virtual comport (COM 34) was created with the parameters given in Table 7. Figure 4.4 shows the screenshot of the CPR Manager, used to create the virtual comport COM 34.

COM 34 Settings	
Item	**Setting**
Host IP Address	192.168.1.105
TCP Port	10001

Table 7: Virtual Comport Settings for COM 34



All Com Ports (5)
Com 1 - 34
Com 1 (Inaccessible)
Com 3 (Inaccessible)
Com 4 (Inaccessible)
Com 23
Com 34

Com 34

Window's Port Name: Lantronix CPR Port (COM34)
Window's Device Name: \Device\CprDevice34
Window's Service Name: CprDrvr
Status: Opened (By another application)

☑ Timeout Reconnect — 0 Reconnect Limit (0 = forever)
☐ Wait on Write — 7 Connection Timeout (in seconds)
☐ Use RFC 2217

DTR: Tie DTR to DCD, DSR always active
Tx Empty: CPR Transmit Buffer Empty

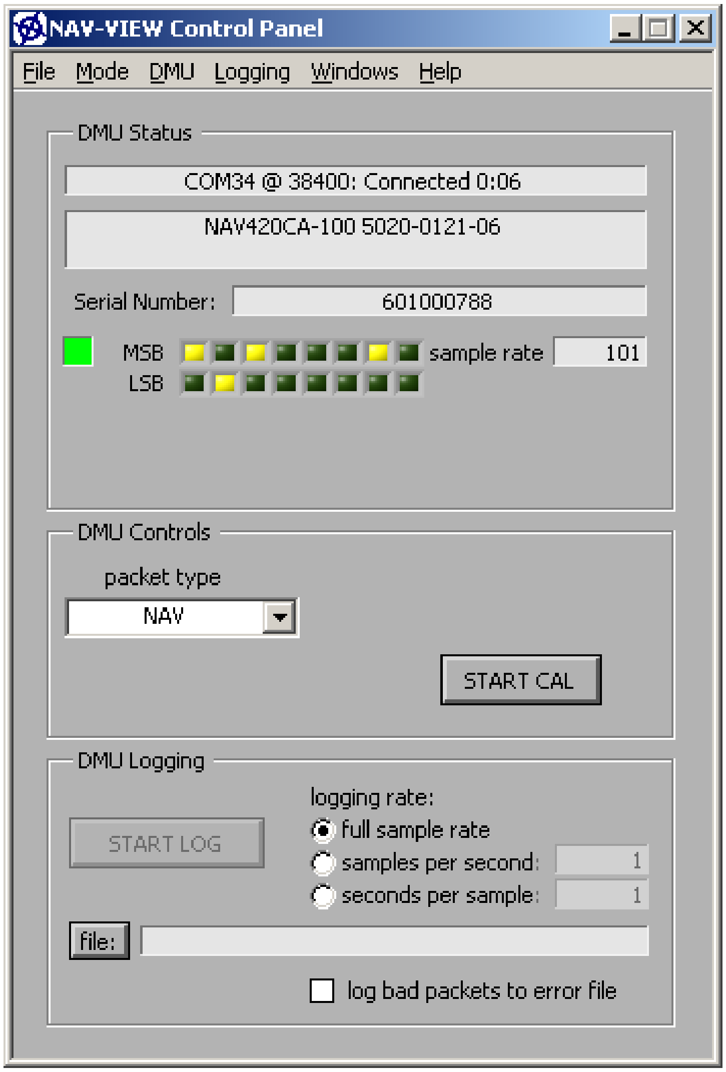
Service	Host	TCP Port
1	192.168.1.105	10001
2		
3		
4		
5		
6		
7		
8		

IP Address	TCP Port	Device Name	Port Name	HW Address	ID	Product
192.168.1.105 (1)	10002	NAV420	10002	00:20:4A:96:63:DC	W7	WiBox BG
192.168.1.105 (2)	10001	NAV420		00:20:4A:96:63:DC	W7	WiBox BG

Changing Names was successful.

Figure 4.4: Screenshot of the CPR Manager

NAV-VIEW, which was installed on the laptop computer detects the virtual comport, COM 34, and connected with it through the wireless adapter. A screenshot of the NAV-VIEW software and the connection summary is given in Figure 4.5.



COM34 @ 38400: Connected 0:06

NAV420CA-100 5020-0121-06

Serial Number: 601000788

sample rate 101

packet type NAV

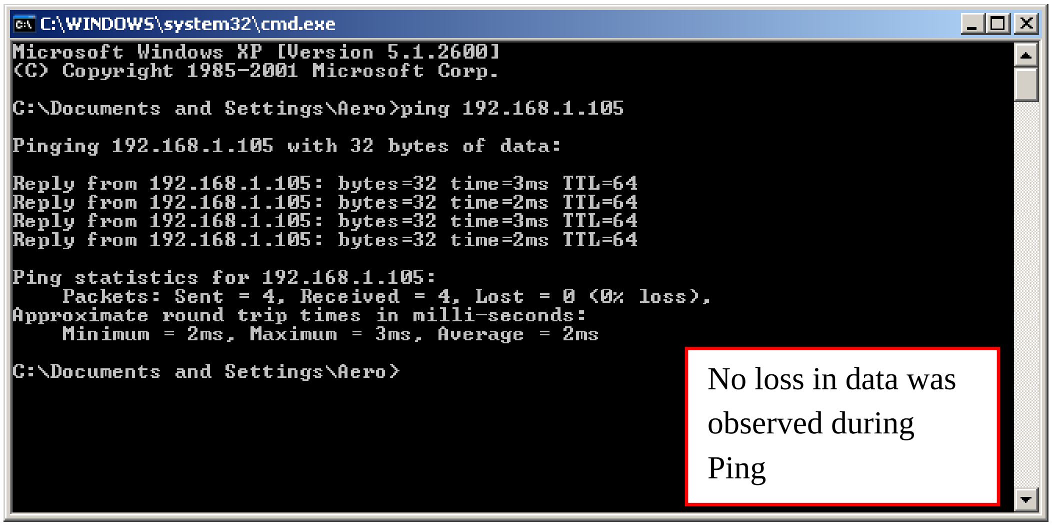
logging rate:
● full sample rate
○ samples per second: 1
○ seconds per sample: 1

□ log bad packets to error file

Figure 4.5: The NAV-VIEW Control Panel

4.1.2. W-AHRS Testing

The testing of the W-AHRS node in the Ad-Hoc mode was accomplished with several tools like ‘Wireshark’, ‘IPTools’ and ‘NetStumbler’. All of these are available as free downloads over the internet under the GNU General Public License. The first method of testing was using the ‘Ping’ command at the command prompt of the user interface node. The result of the ping test for the IP Camera and User Interface Node connection in the wireless mode is shown in Figure 4.6. Initial testing of the wireless connection with ‘Ping’ showed no loss of data and complete signal strength was reflected in the ‘Connection Details’ of the laptop computer. For the ‘Ping’ test, 4 packets of data of 32 bytes each were sent and received with 0% loss and a maximum round trip time of 3 milli-seconds.



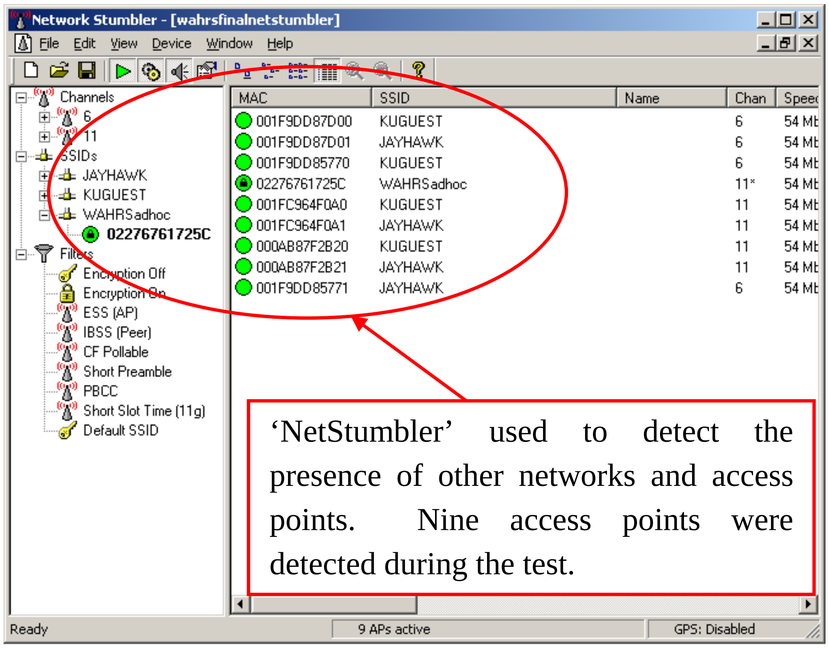
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Aero>ping 192.168.1.105

Pinging 192.168.1.105 with 32 bytes of data:

Reply from 192.168.1.105: bytes=32 time=3ms TTL=64
Reply from 192.168.1.105: bytes=32 time=2ms TTL=64
Reply from 192.168.1.105: bytes=32 time=3ms TTL=64
Reply from 192.168.1.105: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Documents and Settings\Aero>
```

No loss in data was observed during Ping

Figure 4.6: The W-AHRS tested by the Ping Command

After the successful initial testing of the link between the User Interface Node and the W-AHRS by ‘Ping’ and with the connection details established in the User Interface Node, the wireless link was tested using Wireshark, IP Tools and NetStumbler for detailed analysis.

The IEEE 802.11 link between the W-AHRS and the User Interface Node was tested with Wireshark and IP Tools in the presence of multiple networks as identified by NetStumbler. Figure 4.7 shows the screen shot of NetStumbler showing the presence of nine other active access points that were transmitting and are within the connecting range of the User Interface Node. The link of the W-AHRS is also shown in the window along with an indication that the computer running NetStumbler, here the User Interface Node, is connected to this transmitter or node.

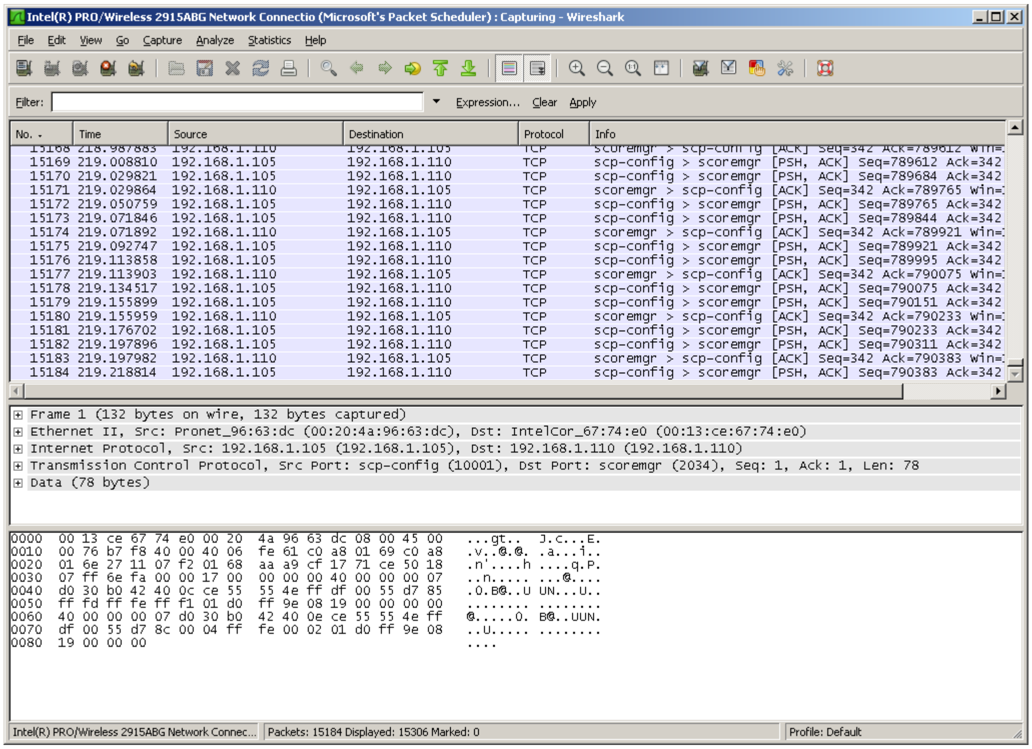


MAC	SSID	Name	Chan	Speed
● 001F9DD87D00	KUGUEST		6	54 Mb
● 001F9DD87D01	JAYHAWK		6	54 Mb
● 001F9DD85770	KUGUEST		6	54 Mb
● 02276761725C	WAHRSadhoc		11*	54 Mb
● 001FC964F0A0	KUGUEST		11	54 Mb
● 001FC964F0A1	JAYHAWK		11	54 Mb
● 000AB87F2B20	KUGUEST		11	54 Mb
● 000AB87F2B21	JAYHAWK		11	54 Mb
● 001F9DD85771	JAYHAWK		6	54 Mb

‘NetStumbler’ used to detect the presence of other networks and access points. Nine access points were detected during the test.

Figure 4.7: Identification of Multiple Access Points within Test Set-up

Figure 4.8 shows the screen shot of the Wireshark tool running during the testing of the wireless link. The test was performed for test duration of 262.120 sec, with 18,072 data packets exchanged over the IEEE 802.11 link, equivalent to 1,924,979 bytes of data captured.


Intel(R) PRO/Wireless 2915ABG Network Connectio (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Intel(R) PRO/Wireless 2915ABG Network Connec...
Packets: 15184 Displayed: 15306 Marked: 0
Profile: Default

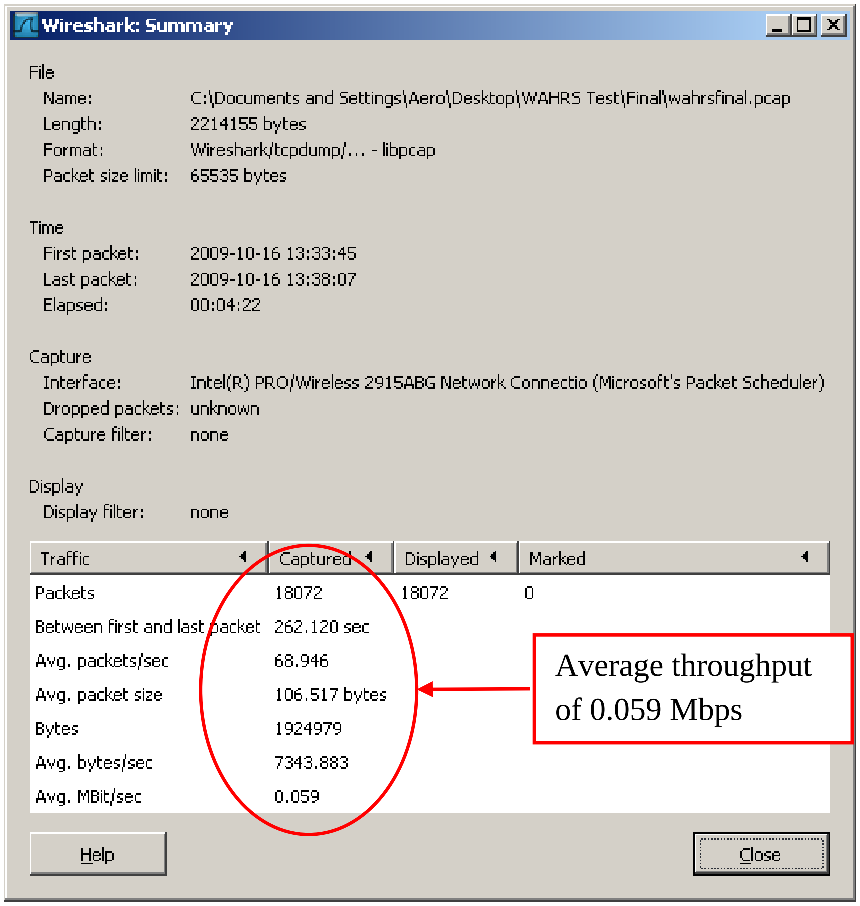
```
No. -  Time        Source          Destination     Protocol  Info
 15168 218.987883 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=789612 Win=
 15169 219.008810 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789612 Ack=342
 15170 219.029821 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789684 Ack=342
 15171 219.029864 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=789765 Win=
 15172 219.050759 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789765 Ack=342
 15173 219.071846 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789844 Ack=342
 15174 219.071892 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=789921 Win=
 15175 219.092747 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789921 Ack=342
 15176 219.113858 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=789995 Ack=342
 15177 219.113903 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=790075 Win=
 15178 219.134517 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=790075 Ack=342
 15179 219.155899 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=790151 Ack=342
 15180 219.155959 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=790233 Win=
 15181 219.176702 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=790233 Ack=342
 15182 219.197896 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=790311 Ack=342
 15183 219.197982 192.168.1.110   192.168.1.105   TCP       scoremgr > scp-config [ACK] Seq=342 Ack=790383 Win=
 15184 219.218814 192.168.1.105   192.168.1.110   TCP       scp-config > scoremgr [PSH, ACK] Seq=790383 Ack=342
```

```
⊞ Frame 1 (132 bytes on wire, 132 bytes captured)
⊞ Ethernet II, Src: Pronet_96:63:dc (00:20:4a:96:63:dc), Dst: IntelCor_67:74:e0 (00:13:ce:67:74:e0)
⊞ Internet Protocol, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.110 (192.168.1.110)
⊞ Transmission Control Protocol, Src Port: scp-config (10001), Dst Port: scoremgr (2034), Seq: 1, Ack: 1, Len: 78
⊞ Data (78 bytes)
```

```
0000  00 13 ce 67 74 e0 00 20  4a 96 63 dc 08 00 45 00   ...gt..  J.c...E.
0010  00 76 b7 f8 40 00 40 06  fe 61 c0 a8 01 69 c0 a8   .v..@.@. .a...i..
0020  01 6e 27 11 07 f2 01 68  aa a9 cf 17 71 ce 50 18   .n'....h ....q.P.
0030  07 ff 6e fa 00 00 17 00  00 00 00 40 00 00 00 07   ..n..... ...@....
0040  d0 30 b0 42 40 0c ce 55  55 4e ff df 00 55 d7 85   .0.B@..U UN...U..
0050  ff fd ff fe ff f1 01 d0  ff 9e 08 19 00 00 00 00   ........ ........
0060  40 00 00 00 07 d0 30 b0  42 40 0e ce 55 55 4e ff   @.....0. B@..UUN.
0070  df 00 55 d7 8c 00 04 ff  fe 00 02 01 d0 ff 9e 08   ..U..... ........
0080  19 00 00 00                                        ....
```

Figure 4.8: Screenshot of 'Wireshark' Taken During the Test

The summary of the test with Wireshark is given in Figure 4.9. Table 8 lists the details of the wireless connection for the individual nodes during the test. An average throughput of 0.059 Mbps was measured. The low throughput of the connection was identified as one of the reasons for the connection being a little less stable. The wireless adapter of the User Interface Node (laptop computer) has the feature to try and connect to a link that is the strongest among the available connections. The data packets were color coded based on the protocol that used for communication. In Figure 4.8, all the data packets were communicated in using the Transmission Control Protocol (TCP) and hence were colored light blue.



File
Name: C:\Documents and Settings\Aero\Desktop\WAHRS Test\Final\wahrsfinal.pcap
Length: 2214155 bytes
Format: Wireshark/tcpdump/... - libpcap
Packet size limit: 65535 bytes

Time
First packet: 2009-10-16 13:33:45
Last packet: 2009-10-16 13:38:07
Elapsed: 00:04:22

Capture
Interface: Intel(R) PRO/Wireless 2915ABG Network Connectio (Microsoft's Packet Scheduler)
Dropped packets: unknown
Capture filter: none

Display
Display filter: none

Traffic	Captured	Displayed	Marked
Packets	18072	18072	0
Between first and last packet	262.120 sec		
Avg. packets/sec	68.946		
Avg. packet size	106.517 bytes		
Bytes	1924979		
Avg. bytes/sec	7343.883		
Avg. MBit/sec	0.059		

Average throughput of 0.059 Mbps

Figure 4.9: Summary of Ad-Hoc Mode Testing of the W-AHRS

Item	**Details**
Address A (W-AHRS)	**192.168.1.105**
Address B (User Interface Node)	**192.168.1.110**
Packets	**18071**
Bytes	**1924937**
Packets A→B	**11994**
Bytes A→B	**1596180**
Packets A←B	**6077**
Bytes A←B	**328757**
Bits per second A→B	**48716.00**
Bits per second A←B	**10033.78**
Duration	**262.1200 sec**

Table 8: Summary for the Individual Nodes

The analysis parameters for the network are: 1) Round Trip Time Graph 2) Throughput Graph and 3) the Time Sequence Graph. These parameters help in the visualization of the performance of the network. Figures 4.10 through 4.12 show the Throughput Graph, Round Trip Time (RTT) Graph and the Time Sequence Graph, respectively, as obtained from Wireshark for the test duration. The Throughput Graph shows a consistent throughput indicative of an interference and congestion free wireless connection. The Round Trip Time Graph, Figure 4.11, with time on y-axis and sequence number on x-axis, indicates a strong signal because of low mean round trip time. It is also indicative of an interference free connection.

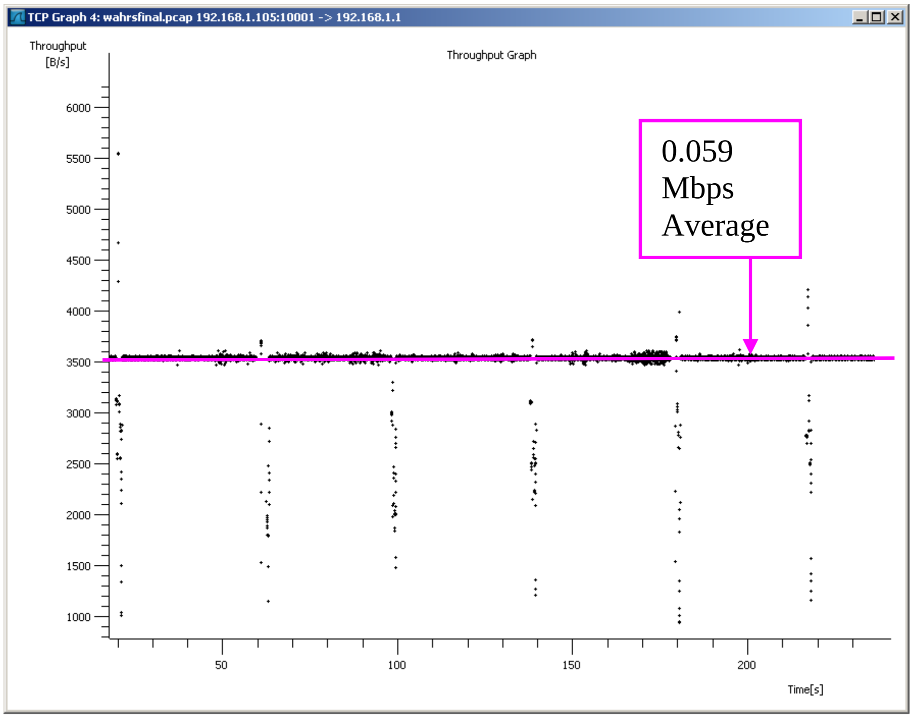


Figure 4.10: Throughput Graph of the W-AHRS Testing

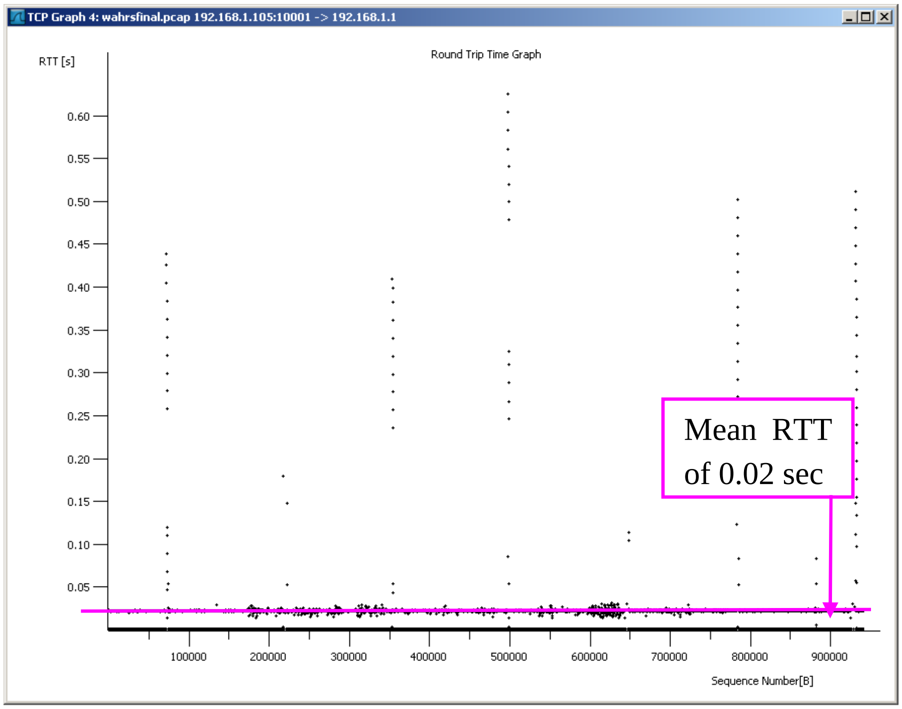


Figure 4.11: Round Trip Time Graph for the IP Camera Testing

The Time Sequence Graph, with Sequence Number on the Y-axis and Time on the X-axis is used to check the network using the sequence numbers assigned to the data packets during transmission. A steady Time Sequence Graph shows that the connection is without data loss.

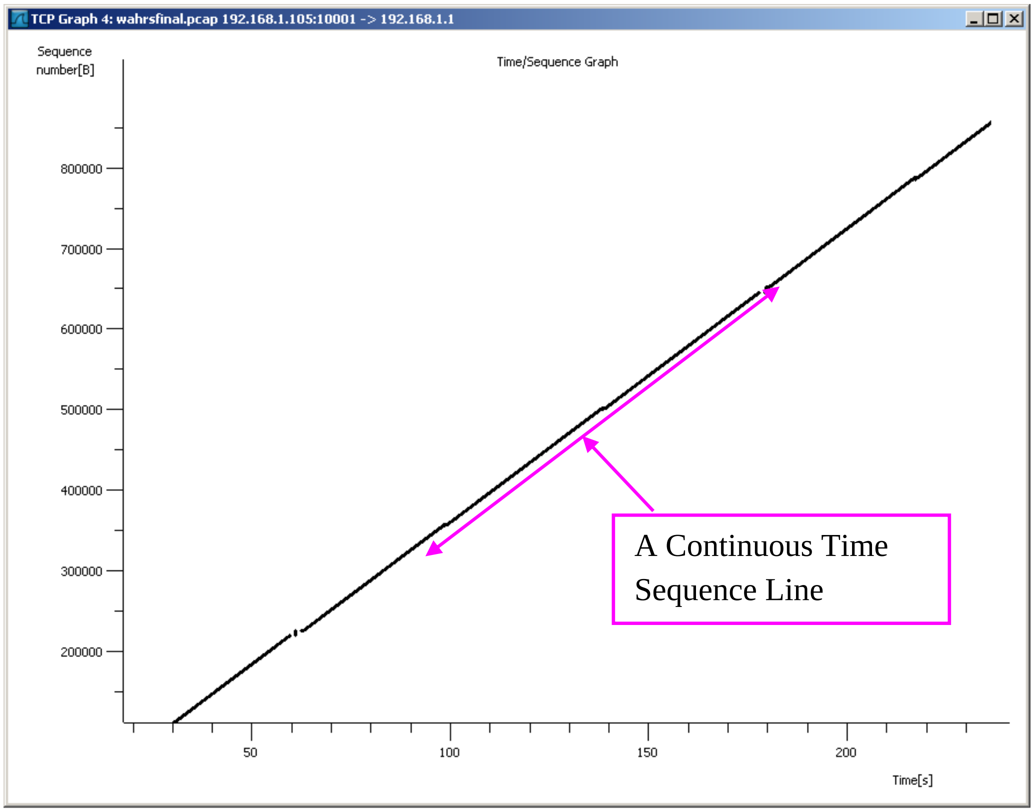


Figure 4.12: Time Sequence Graph for the IP Camera Testing

Wireshark is a packet sniffer tool that is used for network trouble shooting, communication protocol identification and development. For the graphical presentation and analysis of the communication protocols here, IP Tools was used. The results obtained using IP Tools for testing the link between the IP Camera and the user Interface Node are given in Figures 4.13 through 4.16. The test was conducted for a duration of 214.703 seconds with 14,858 data packets captured, equivalent to 1,581,050 bytes of data at an average of 0.059 Mbits/sec.

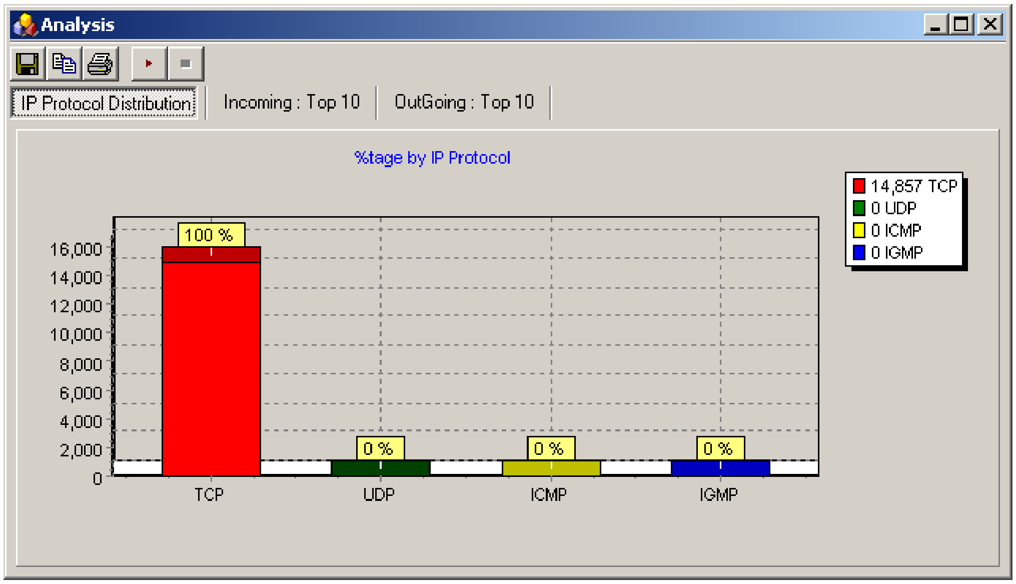


Figure 4.13: Internet Protocol Summary for Testing of W-AHRS using 'IPTools'

Figure 4.13 shows that the connection between the W-AHRS and the User Interface Node was based on the Transmission Control Protocol. This implies that the connection is secure by choice of protocol as well. No data was lost because of the inherent characteristics of the TCP/IP Protocol. In the User Datagram Protocol there is no acknowledgement of the receipt of a data packet to the transmitter and hence there is a chance that data is being lost as there is no check to acknowledge receipt of a transmission. In the TCP protocol, there is always an acknowledgement for a data packet transmitted and hence data is not lost unless the connection is lost. If the data is lost, it is retransmitted.

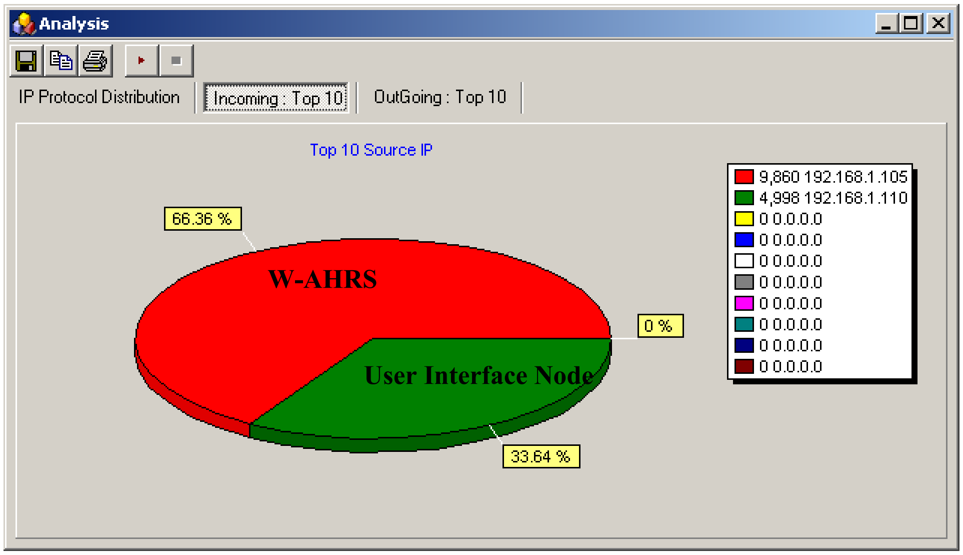


Figure 4.14: Source IP Address during Testing of W-AHRS by 'IPTools'

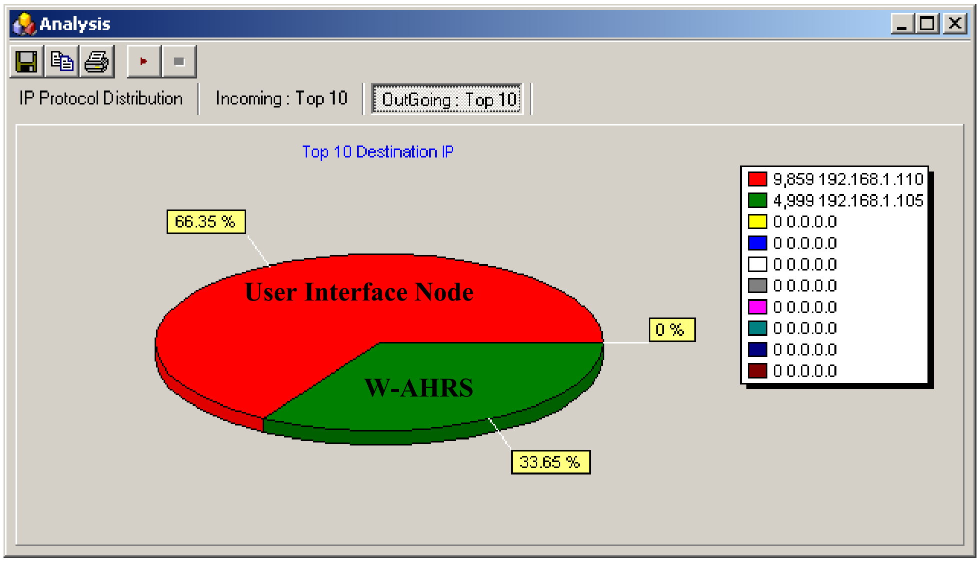
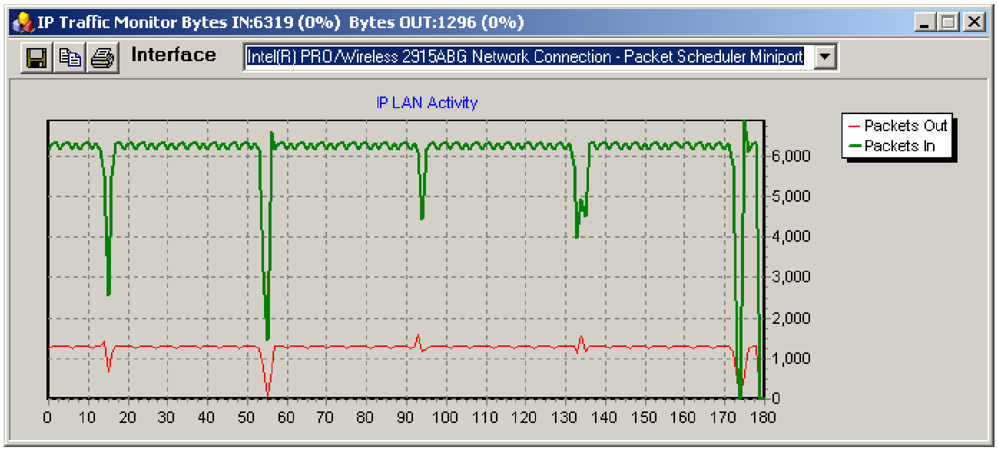


Figure 4.15: Destination IP Address during Testing of W-AHRS by 'IPTools'

Figures 4.14 and 4.15 show the source and destination IP addresses of the nodes that participated in the network. The W-AHRS is the major source, transmitting 66.36% of the connection time. The User Interface Node is the major destination, receiving data 63.5% of the connection time. No other IP addresses participated in the network, an indication that the network was free from interference and that the wireless link was secure. The same result is also verified by the IP LAN Activity graph, given in Figure 4.16. In this graph, it is evident that the major LAN activity during this test was the W-AHRS transmitting data and the user interface node acknowledging the same.



IP Traffic Monitor Bytes IN:6319 (0%) Bytes OUT:1296 (0%)

Interface: Intel(R) PRO/Wireless 2915ABG Network Connection - Packet Scheduler Miniport

Figure 4.16: IP LAN Activity for the W-AHRS Test

NetStumbler was also used to measure the signal-to-noise ratio of the IEEE 802.11 link between the IP Camera and the user interface node. It showed a consistently strong signal.

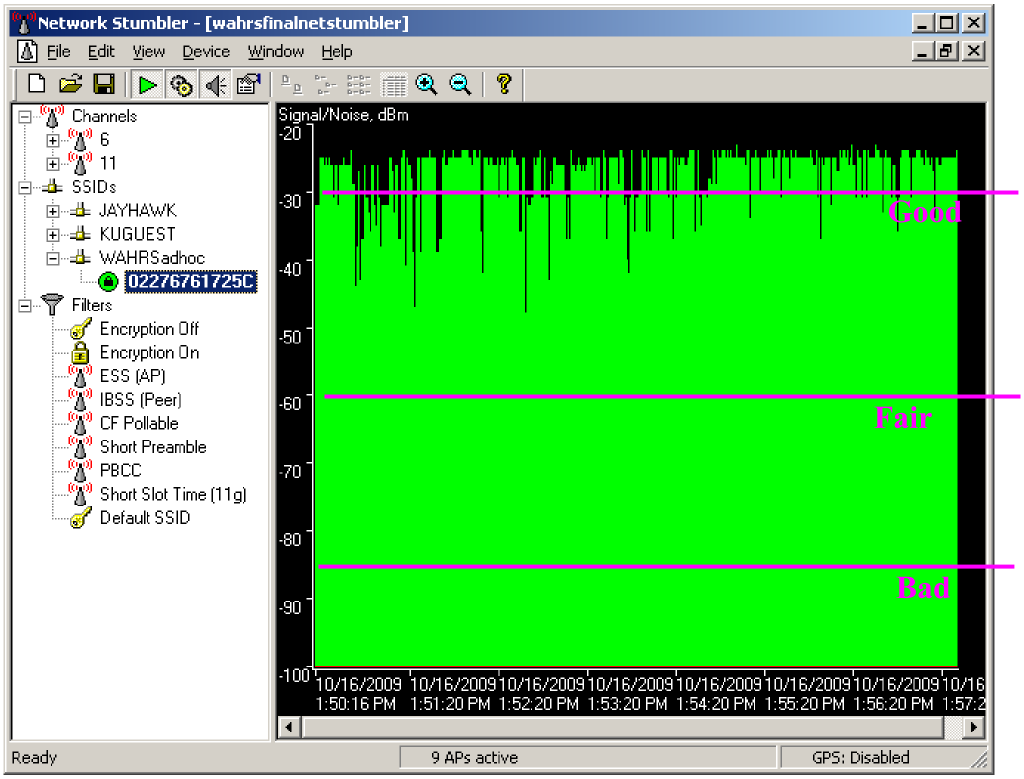


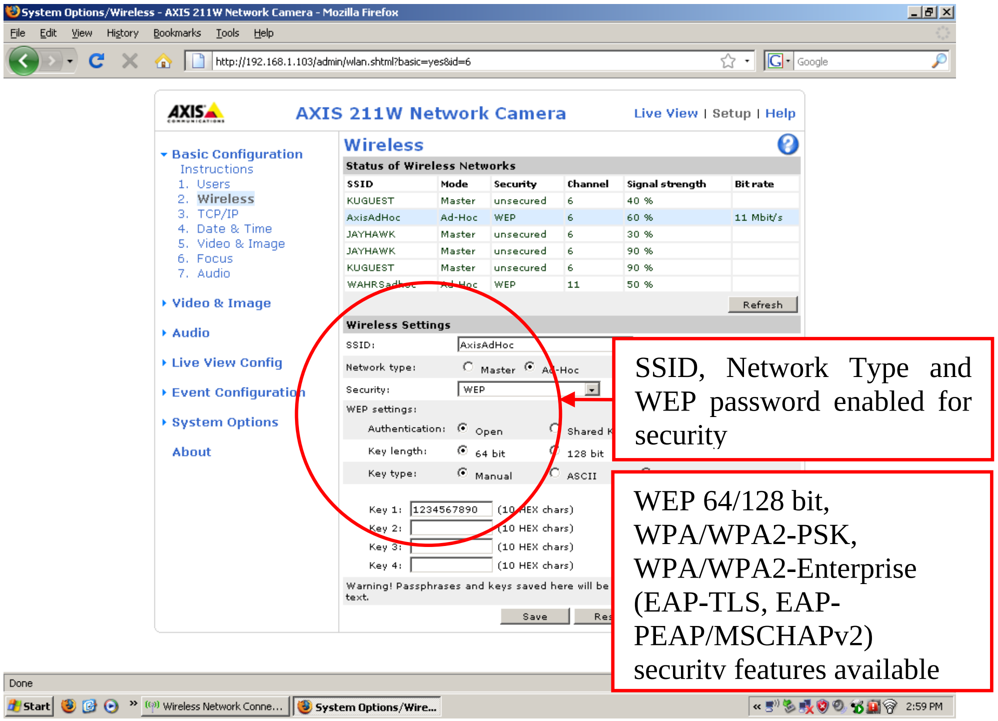
Figure 4.17: Signal to Noise Ratio for the W-AHRS Connection

4.2. IP Camera in Ad-Hoc Mode

Ad-Hoc mode testing of the IP Camera permitted testing the IEEE 802.11 b/g protocols for data intensive applications like video recording. In this section, the configuration and testing of the IP Camera in the Ad-Hoc mode are described.

4.2.1. Configuring the IP Camera

The IP Camera was configured by accessing the device through an Ethernet Cross-Over Cable. The camera must be initially configured through a wired connection and can later be configured by accessing it wirelessly. During the initial wired configuration of the IP Camera, the master credentials for accessing the device and the administrative privileges were set. For our device, the master credentials were set to Login ID: *root* with Password: *ADMRC123*. With this login and password, the user can reconfigure the device even while accessing it wirelessly. The procedure to reconfigure the device without these credentials will be to reset the IP Camera to the factory default settings and then re-assigning the administrative password.



Wireless

Status of Wireless Networks

SSID	Mode	Security	Channel	Signal strength	Bit rate
KUGUEST	Master	unsecured	6	40 %	
AxisAdHoc	Ad-Hoc	WEP	6	60 %	11 Mbit/s
JAYHAWK	Master	unsecured	6	30 %	
JAYHAWK	Master	unsecured	6	90 %	
KUGUEST	Master	unsecured	6	90 %	
WAHRSadhoc	Ad-Hoc	WEP	11	50 %	

Wireless Settings

SSID: AxisAdHoc

Network type: ○ Master ● Ad-Hoc

Security: WEP

WEP settings:

Authentication: ● Open ○ Shared K

Key length: ● 64 bit ○ 128 bit

Key type: ● Manual ○ ASCII

Key 1: 1234567890 (10 HEX chars)

Key 2: (10 HEX chars)

Key 3: (10 HEX chars)

Key 4: (10 HEX chars)

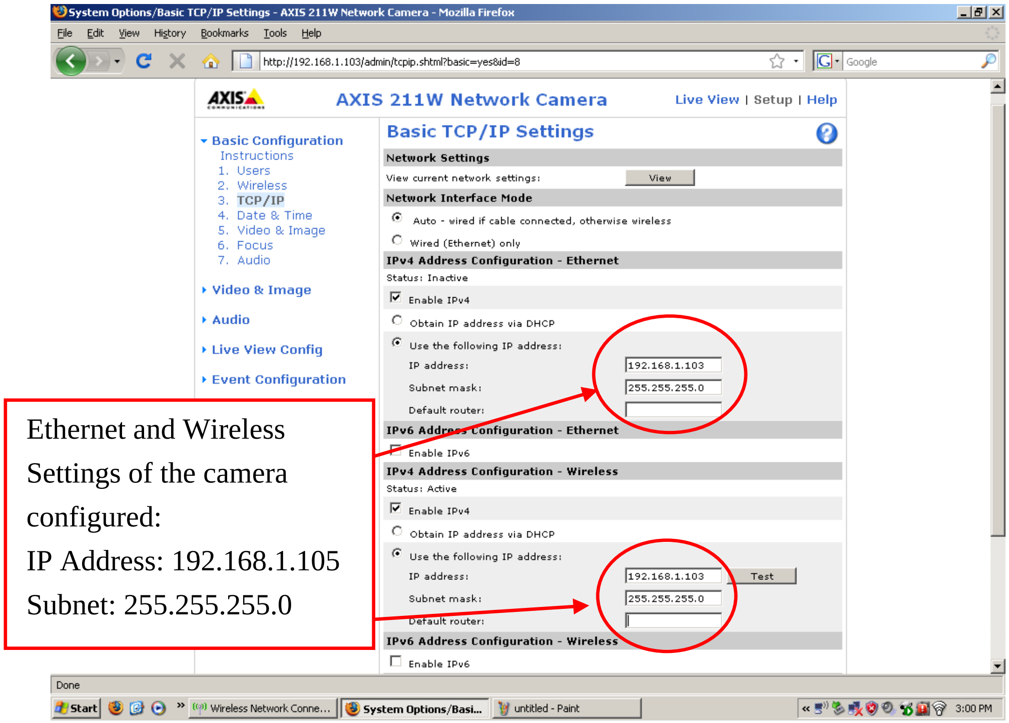
Warning! Passphrases and keys saved here will be text.

SSID, Network Type and WEP password enabled for security

WEP 64/128 bit, WPA/WPA2-PSK, WPA/WPA2-Enterprise (EAP-TLS, EAP-PEAP/MSCHAPv2) securitv features available

Figure 4.18: Wireless Configuration of the IP Camera

Figure 4.18 and Figure 4.19 show the screenshots of the configuration pages of the IP Camera, when accessed via a web browser using its assigned IP address. For the Ad-Hoc mode inclusion and testing of the IP Camera, the details of its configuration are summarized in Table 9. With the settings given in Table 10, the IP Camera was configured in the Ad-Hoc mode with the User Interface Node (laptop computer), as shown in Figure 4.20. The testing and evaluation of the IP Camera in the Ad-Hoc mode and the test results are presented in the next section.



Basic TCP/IP Settings

Network Settings

View current network settings:

Network Interface Mode

● Auto - wired if cable connected, otherwise wireless

○ Wired (Ethernet) only

IPv4 Address Configuration - Ethernet

Status: Inactive

☑ Enable IPv4

○ Obtain IP address via DHCP

● Use the following IP address:

IP address: 192.168.1.103

Subnet mask: 255.255.255.0

Default router:

IPv6 Address Configuration - Ethernet

☐ Enable IPv6

IPv4 Address Configuration - Wireless

Status: Active

☑ Enable IPv4

○ Obtain IP address via DHCP

● Use the following IP address:

IP address: 192.168.1.103

Subnet mask: 255.255.255.0

Default router:

IPv6 Address Configuration - Wireless

☐ Enable IPv6

Ethernet and Wireless Settings of the camera configured:
IP Address: 192.168.1.105
Subnet: 255.255.255.0

Figure 4.19: Configuring the TCP/IP Settings of the IP Camera

Wireless Network Settings	
Item	**Setting**
Wireless Network Name or SSID	AxisAdHoc
Channel Scan	Enabled
Security Mode	WEP Enabled
Network Mode	Ad-Hoc
Network Name	ADMRCIPCAM
Security Settings	
Item	**Setting**
Authentication	Open
WEP Encryption	64 bit
Key Type	HEX
WEP Key 1	1234567890(needs to be 10 characters long)

Table 9: Wireless and Security Settings of the IP Camera

Basic TCP/IP Settings	
Item	**Setting**
IP Address	192.168.001.105
Gateway IP Address	0.0.0.0
Subnet Mask	255.255.255.0

Table 10: TCP/IP Settings of the IP Camera

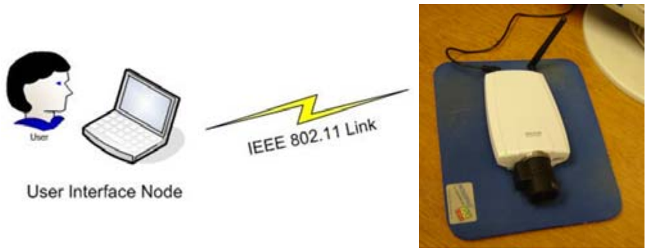


Figure 4.20: Video Node in Ad-Hoc Mode with User Interface Node

Mode: Ad-Hoc
SSID: AxisAdHoc
WEP: 64 bit
Channel: 11
Band: IEEE 802.11 g

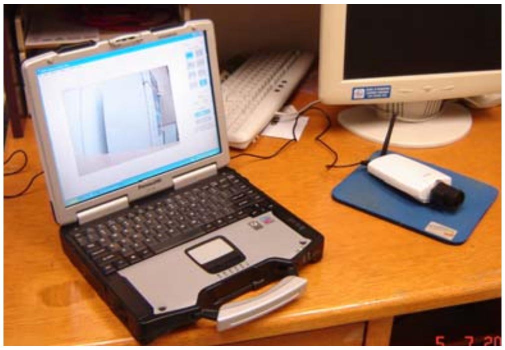
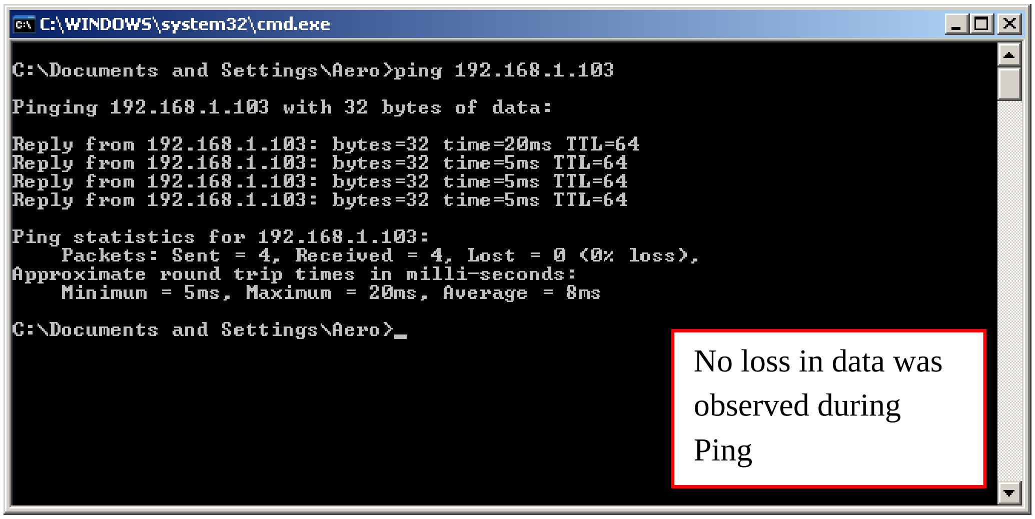


Figure 4.21: IP Camera in Ad-Hoc Mode with User Interface Node

4.2.2. Video Node Testing

The connection between the User Interface Node and the IP Camera was first tested by using the ‘Ping’ command. At the command prompt, pinging a particular IP Address enables evaluation of the connection status. The result of the ping test for the IP Camera and User Interface Node connection in the wireless mode is shown in Figure 4.22. Initial testing of the wireless connection with ‘Ping’ showed no loss of data and complete signal strength was reflected in the ‘Connection Details’ of the laptop computer. For the ‘ping’ test, 4 packets of data of 32 bytes each were sent and received with 0% loss and a maximum round trip time of 20 milli-seconds.

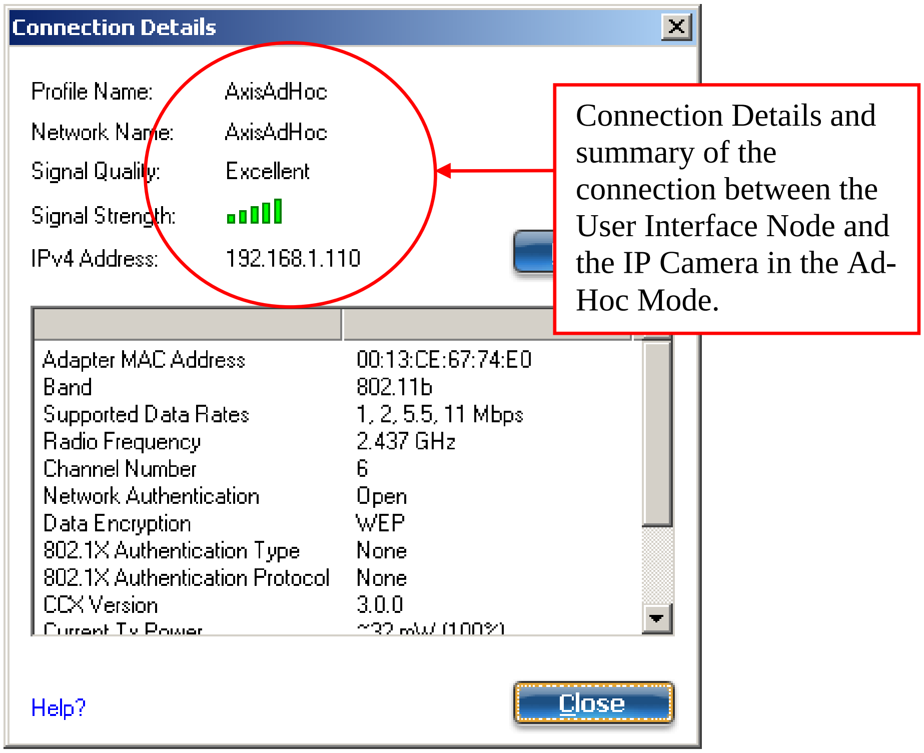


```
C:\Documents and Settings\Aero>ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:

Reply from 192.168.1.103: bytes=32 time=20ms TTL=64
Reply from 192.168.1.103: bytes=32 time=5ms TTL=64
Reply from 192.168.1.103: bytes=32 time=5ms TTL=64
Reply from 192.168.1.103: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 20ms, Average = 8ms

C:\Documents and Settings\Aero>_
```

No loss in data was observed during Ping

Figure 4.22: The IP Camera Tested by the Ping Command

The strength of the connection was also observed when configuring the User Interface Node to connect to the IP Camera. The wireless connection details of the User Interface Node are shown in Figure 4.23.



Connection Details

Profile Name: AxisAdHoc

Network Name: AxisAdHoc

Signal Quality: Excellent

Signal Strength: ▂▃▄▅▆

IPv4 Address: 192.168.1.110

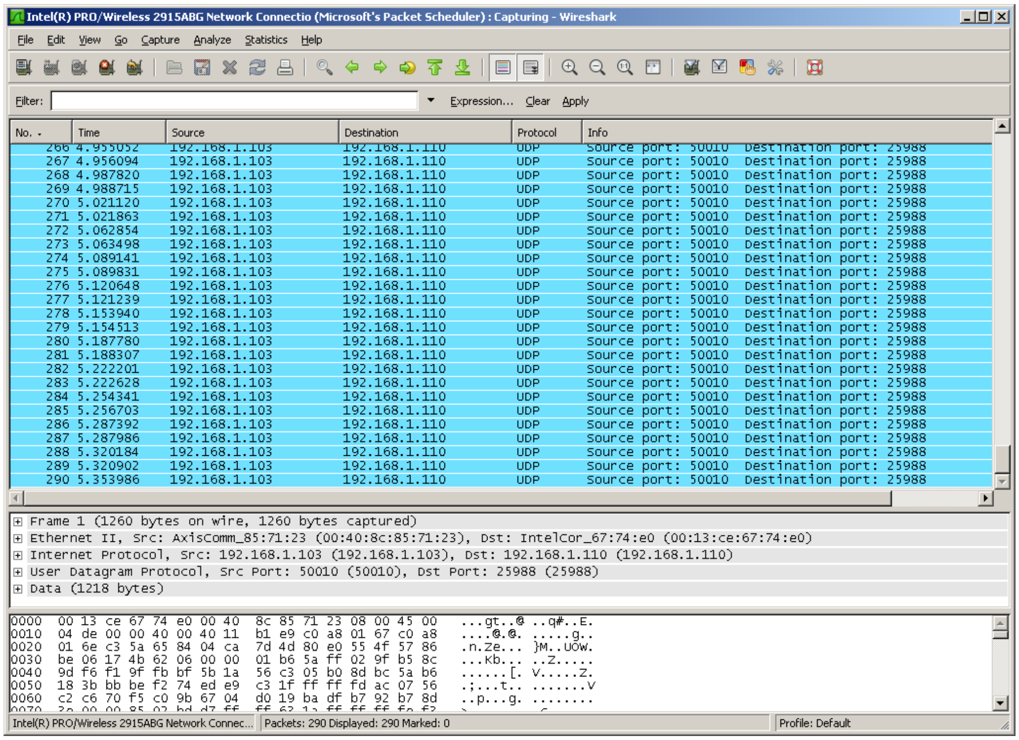
Adapter MAC Address	00:13:CE:67:74:E0
Band	802.11b
Supported Data Rates	1, 2, 5.5, 11 Mbps
Radio Frequency	2.437 GHz
Channel Number	6
Network Authentication	Open
Data Encryption	WEP
802.1X Authentication Type	None
802.1X Authentication Protocol	None
CCX Version	3.0.0
Current Tx Power	~32 mW (100%)

Connection Details and summary of the connection between the User Interface Node and the IP Camera in the Ad-Hoc Mode.

Figure 4.23: Connection Details (Ad-Hoc) Mode

After the successful initial testing of the link between the User Interface Node and the IP Camera by ‘Ping’ and with the connection details as shown in the User Interface Node, the wireless link was tested using Wireshark, IP Tools and NetStumbler for detailed analysis.

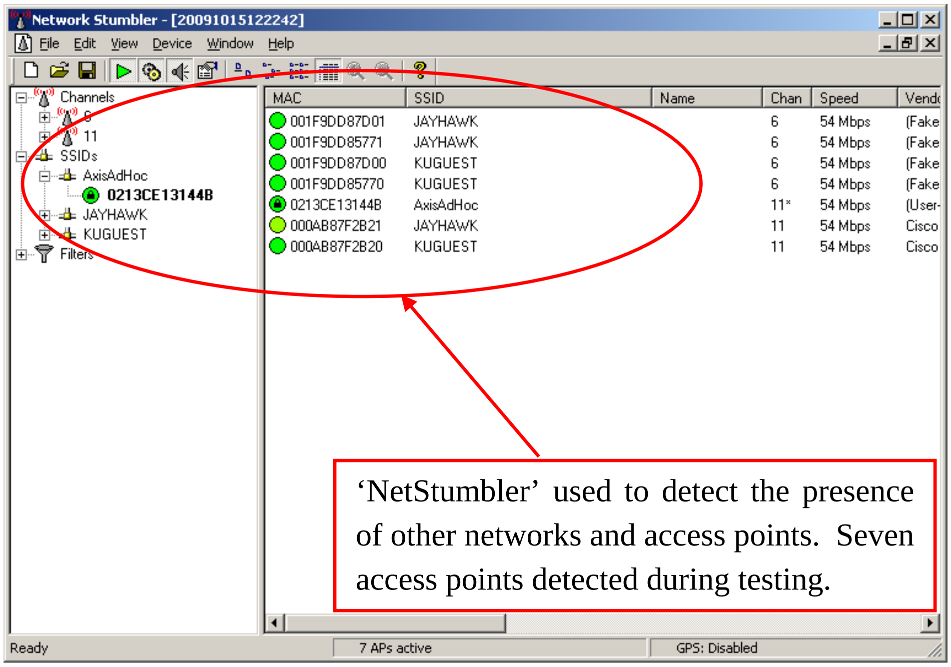
Figure 4.24 shows the screen shot of the Wireshark tool running during the testing of the wireless link. The data packets are color coded in cyan shade to indicate that the UDP protocol was used for the communication. The test was performed for test duration of 500.884 seconds, with 26,880 data packets exchanged over the IEEE 802.11 link, equivalent to 31,855,362 bytes of captured data.


Intel(R) PRO/Wireless 2915ABG Network Connectio (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time        Source          Destination     Protocol  Info
  266 4.955052    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  267 4.956094    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  268 4.987820    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  269 4.988715    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  270 5.021120    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  271 5.021863    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  272 5.062854    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  273 5.063498    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  274 5.089141    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  275 5.089831    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  276 5.120648    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  277 5.121239    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  278 5.153940    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  279 5.154513    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  280 5.187780    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  281 5.188307    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  282 5.222201    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  283 5.222628    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  284 5.254341    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  285 5.256703    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  286 5.287392    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  287 5.287986    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  288 5.320184    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  289 5.320902    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988
  290 5.353986    192.168.1.103   192.168.1.110   UDP       Source port: 50010  Destination port: 25988

⊞ Frame 1 (1260 bytes on wire, 1260 bytes captured)
⊞ Ethernet II, Src: AxisComm_85:71:23 (00:40:8c:85:71:23), Dst: IntelCor_67:74:e0 (00:13:ce:67:74:e0)
⊞ Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 192.168.1.110 (192.168.1.110)
⊞ User Datagram Protocol, Src Port: 50010 (50010), Dst Port: 25988 (25988)
⊞ Data (1218 bytes)

0000  00 13 ce 67 74 e0 00 40  8c 85 71 23 08 00 45 00   ...gt..@ ..q#..E.
0010  04 de 00 00 40 00 40 11  b1 e9 c0 a8 01 67 c0 a8   ....@.@. .....g..
0020  01 6e c3 5a 65 84 04 ca  7d 4d 80 e0 55 4f 57 86   .n.Ze... }M..UOW.
0030  be 06 17 4b 62 06 00 00  01 b6 5a ff 02 9f b5 8c   ...Kb... ..Z.....
0040  9d f6 f1 9f fb bf 5b 1a  56 c3 05 b0 8d bc 5a b6   ......[. V.....Z.
0050  18 3b bb be f2 74 ed e9  c3 1f ff ff fd ac 07 56   .;...t.. .......V
0060  c2 c6 70 f5 c0 9b 67 04  d0 19 ba df b7 92 b7 8d   ..p...g. ........

Intel(R) PRO/Wireless 2915ABG Network Connec...   Packets: 290 Displayed: 290 Marked: 0   Profile: Default
```

Figure 4.24: Screenshot of 'Wireshark' taken during the Test

The IEEE 802.11 link between the IP Camera and the User Interface Node was tested with Wireshark and IP Tools in the presence of multiple networks as identified by NetStumbler. Figure 4.25 shows the screen shot of NetStumber showing the presence of seven other active access points that are transmitting and are within the connecting range of the User Interface Node. The link of the IP Camera is also shown in the window along with an indication that the computer running NetStumbler, here the User Interface Node is connected to this transmitter or node.

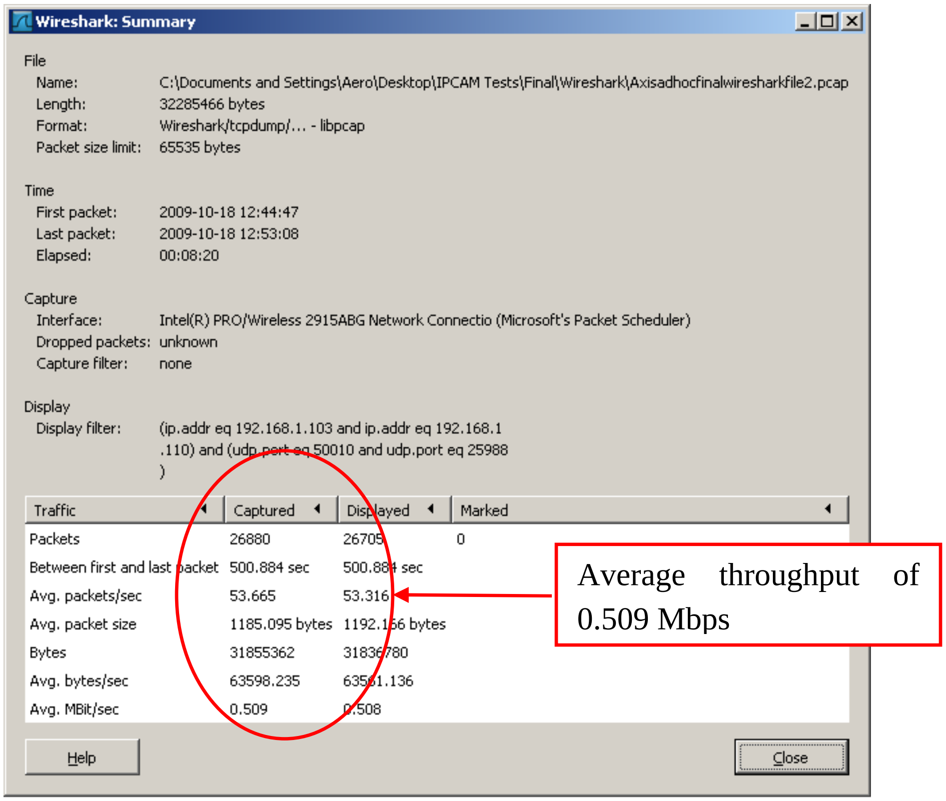


MAC	SSID	Name	Chan	Speed	Vend
● 001F9DD87D01	JAYHAWK		6	54 Mbps	(Fake
● 001F9DD85771	JAYHAWK		6	54 Mbps	(Fake
● 001F9DD87D00	KUGUEST		6	54 Mbps	(Fake
● 001F9DD85770	KUGUEST		6	54 Mbps	(Fake
● 0213CE13144B	AxisAdHoc		11*	54 Mbps	(User-
● 000AB87F2B21	JAYHAWK		11	54 Mbps	Cisco
● 000AB87F2B20	KUGUEST		11	54 Mbps	Cisco

'NetStumbler' used to detect the presence of other networks and access points. Seven access points detected during testing.

Figure 4.25: Identification of Multiple Access Points within Test Set-up

The summary of the testing with Wireshark is given in Figure 4.26, below. An average throughput of 0.509 Mbps was tested. This, when compared to the earlier throughput of about 0.059 Mbps measured with the Wireless AHRS node is a substantial leap and also supports the idea of appropriate bandwidth utilization available with the IEEE 802.11 link through the video node. The details of the connection and the transmissions from the individual nodes are given in Table 11.



Wireshark: Summary

```
File
  Name:             C:\Documents and Settings\Aero\Desktop\IPCAM Tests\Final\Wireshark\Axisadhocfinalwiresharkfile2.pcap
  Length:           32285466 bytes
  Format:           Wireshark/tcpdump/... - libpcap
  Packet size limit: 65535 bytes

Time
  First packet:     2009-10-18 12:44:47
  Last packet:      2009-10-18 12:53:08
  Elapsed:          00:08:20

Capture
  Interface:        Intel(R) PRO/Wireless 2915ABG Network Connectio (Microsoft's Packet Scheduler)
  Dropped packets:  unknown
  Capture filter:   none

Display
  Display filter:   (ip.addr eq 192.168.1.103 and ip.addr eq 192.168.1
                    .110) and (udp.port eq 50010 and udp.port eq 25988
                    )
```

Traffic	Captured	Displayed	Marked
Packets	26880	26705	0
Between first and last packet	500.884 sec	500.884 sec	
Avg. packets/sec	53.665	53.316	
Avg. packet size	1185.095 bytes	1192.156 bytes	
Bytes	31855362	31836780	
Avg. bytes/sec	63598.235	63561.136	
Avg. MBit/sec	0.509	0.508	

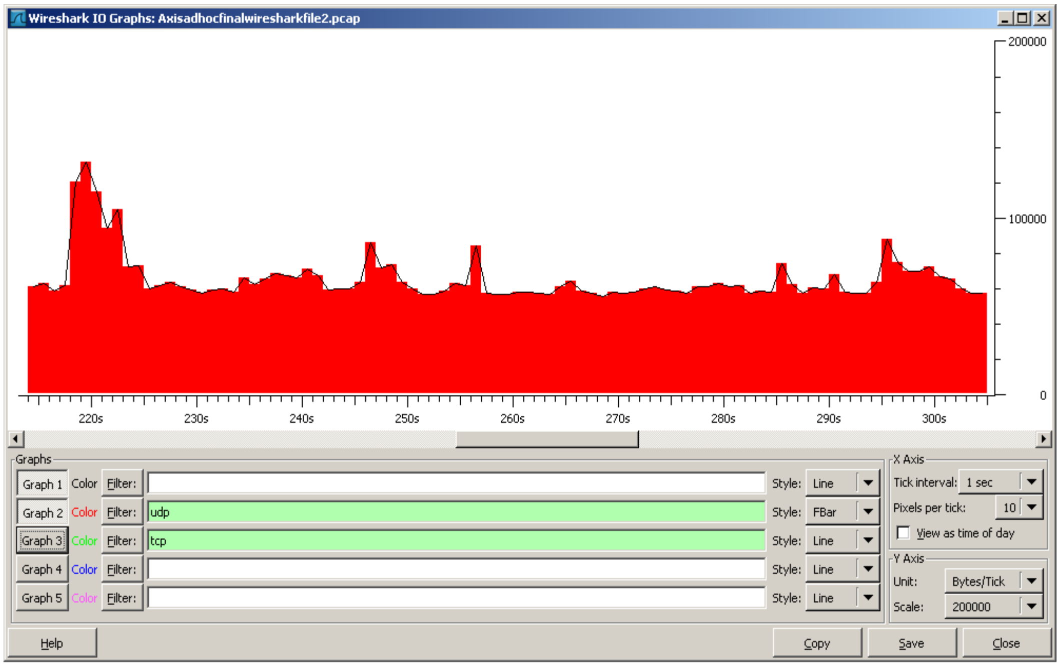
Average throughput of 0.509 Mbps

Figure 4.26: Summary of Ad-Hoc Mode Testing of the IP Camera

Item	**Details**
Address A (IP Camera)	**192.168.1.103**
Address B (User Interface Node)	**192.168.1.110**
Packets	**26862**
Bytes	**31854606**
Packets A→B	**268226**
Bytes A→B	**31850388**
Packets A←B	**36**
Bytes A←B	**4218**
Bits per second A→B	**508706.43**
Bits per second A←B	**67.37**
Duration	**500.884 sec**

Table 11: Details of Wireshark Test of IP Camera in Ad-Hoc Mode

The transmissions from the IP Camera were made using the UDP protocol for video transmission over the IEEE 802.11 g link. In this protocol, analysis parameters like Round Trip Time, Throughput and the Time Sequence Graph are not measured. These parameters are measured only for communications using the Transmission Control Protocol, because, unlike the UDP, it requires an acknowledgment for successful data transmission and measurement of the parameters. The I/O graph for the connection between the IP Camera and the user interface node is given in Figure 4.27. It shows that the connection was based completely on the UDP protocol and it also shows that the connection was secure and no interference from other access points present in the vicinity affected or participated in the connection.



Wireshark IO Graphs: Axisadhocfinalwiresharkfile2.pcap

Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: udp Style: FBar
Graph 3 Color Filter: tcp Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line

X Axis
Tick interval: 1 sec
Pixels per tick: 10
□ View as time of day

Y Axis
Unit: Bytes/Tick
Scale: 200000

Figure 4.27: I/O Graph for the IP Camera

The graphical presentation and analysis of the communication protocols was obtained using IP Tools. The results obtained using IP Tools for tests of the link between the IP Camera and the user Interface Node are given in Figures 4.28 through 4.31. The test duration was 349.024 seconds, during which 16,762 packets of data equivalent to 20,008,521 bytes was captured.

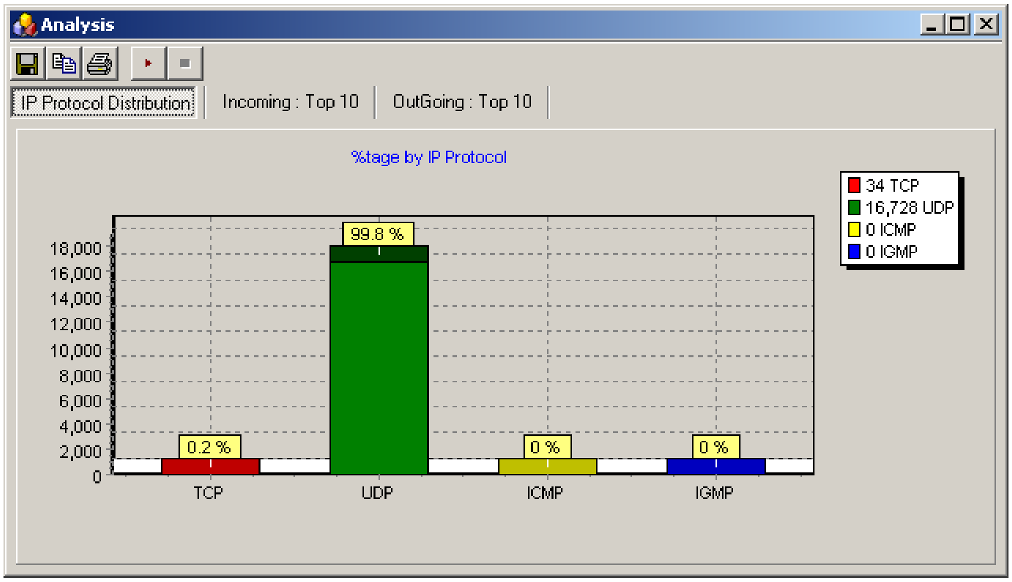


Figure 4.28: Internet Protocol Summary for testing of IP Camera by 'IPTools'

Figure 4.28 shows that the connection between the IP Camera and the User Interface Node was based on the UDP protocol. The UDP Protocol is used where there is no requirement to confirm that a data packet has been received by the receiver node, as in our case. The video from the video camera can be recorded on the user interface node. When using the TCP protocol there is always an acknowledgement for a data packet transmitted and hence data is not lost unless the connection is lost.

Figure 4.29 and Figure 4.30 shows the source and destination IP addresses of the nodes that participated in the network. The IP camera is the only source, transmitting 99.87% of the connection time. The user interface node is the only destination, receiving data 99.87% of the connection time. No other IP addresses participated in the network, an indication that the network was free from interference and that the wireless link was secure. The same result is also verified by the IP LAN Activity graph, given in Figure 4.31. In this graph, it is evident that the major LAN activity during this test was the IP Camera transmitting data.

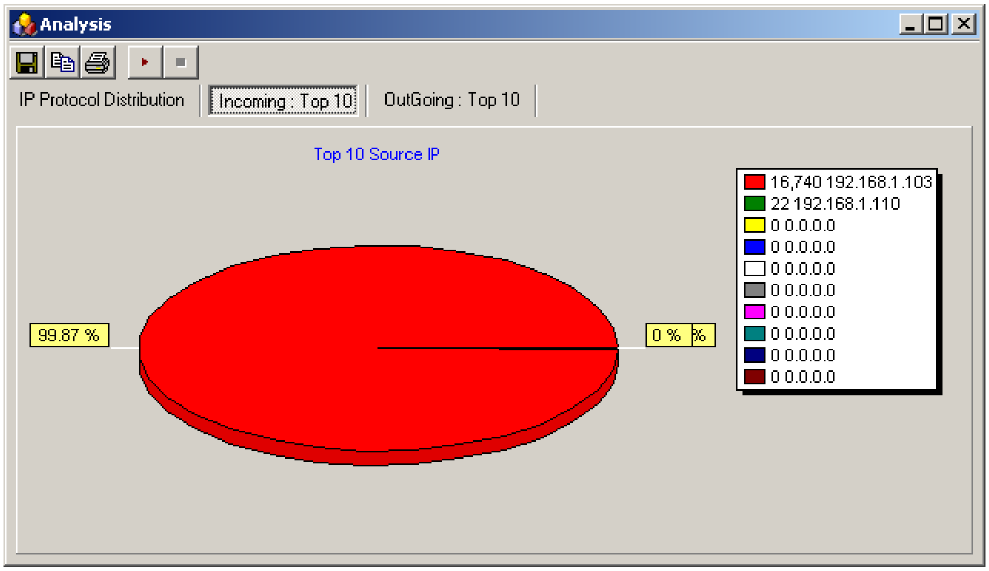


Figure 4.29: Source IP Address during testing of IP Camera by ‘IPTools’

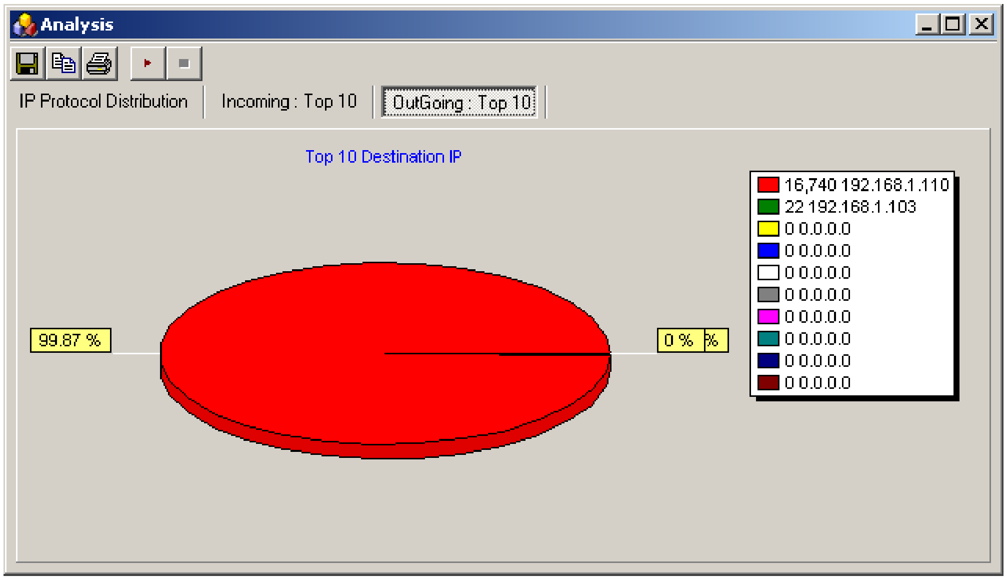
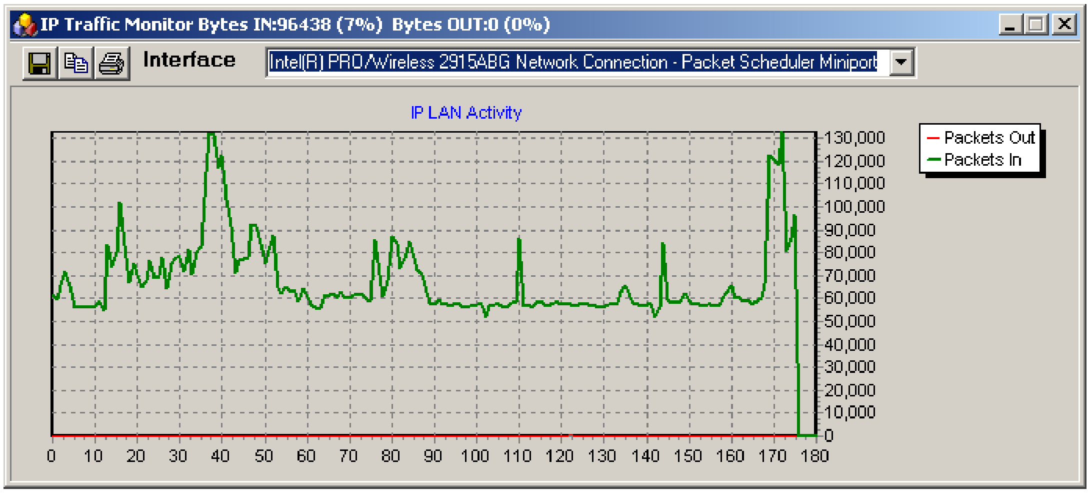


Figure 4.30: Destination IP Address during testing of IP Camera by 'IPTools'



IP Traffic Monitor Bytes IN:96438 (7%) Bytes OUT:0 (0%)

Interface Intel(R) PRO/Wireless 2915ABG Network Connection - Packet Scheduler Miniport

Figure 4.31: IP LAN Activity for the IP Camera Test

NetStumbler was also used to measure the signal-to-noise ratio of the IEEE 802.11 link between the IP Camera and the user interface node. It showed a consistently strong signal, as shown in Figure 4.32.

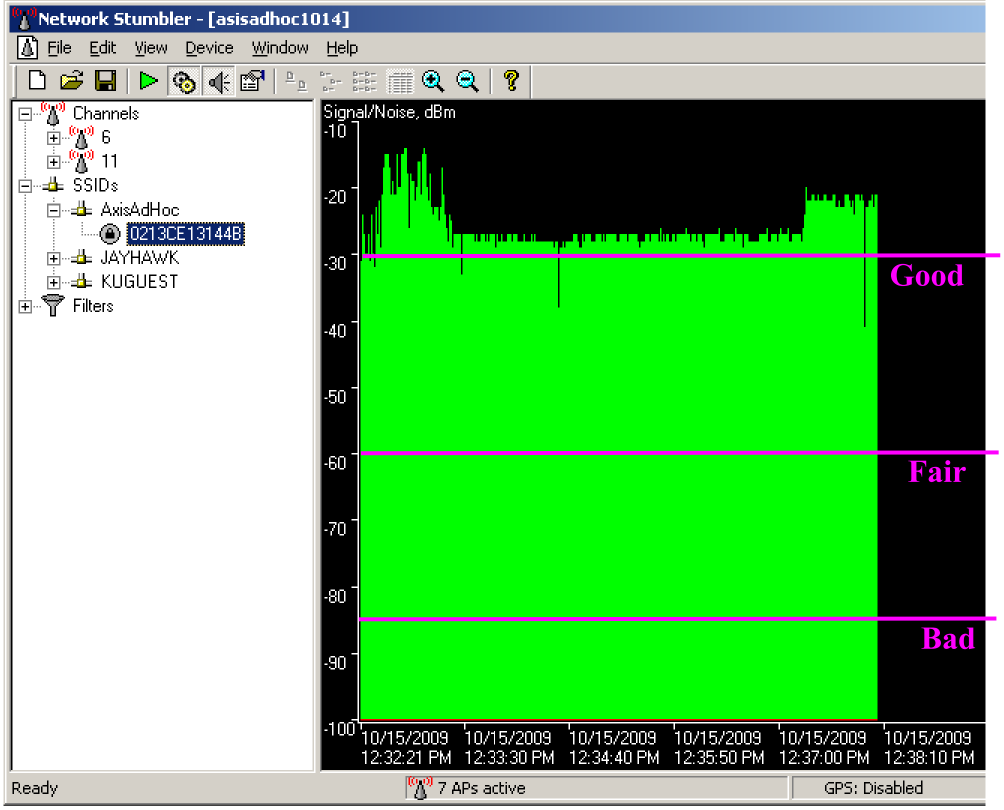


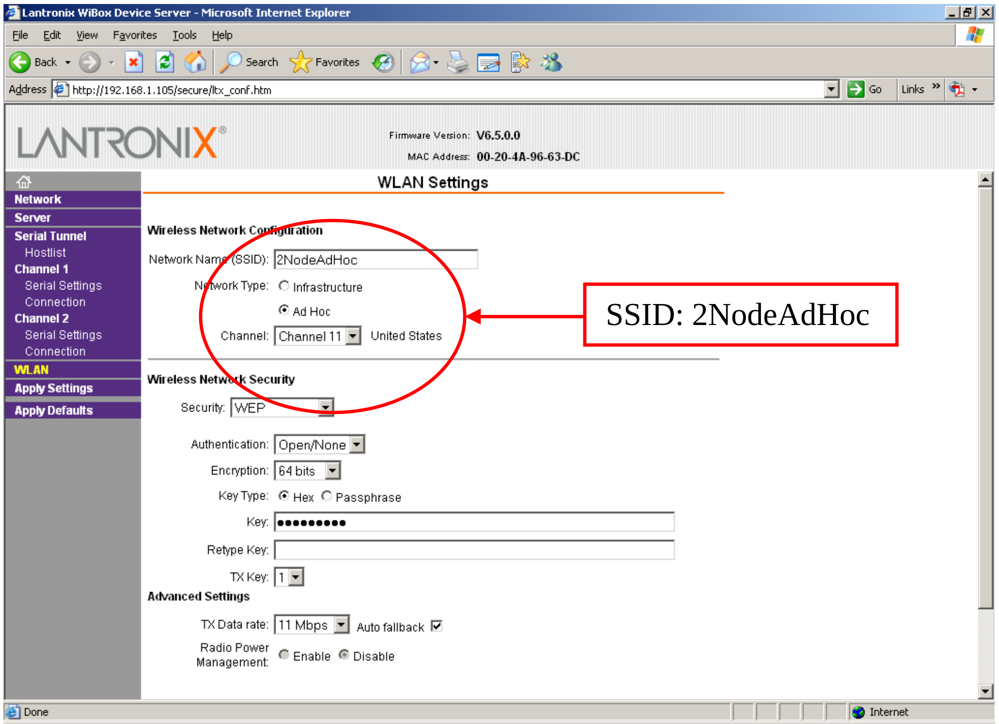
Figure 4.32: Signal to Noise Ratio for the IP Camera

4.3. Three Nodes in Ad-Hoc Mode

The testing of the W-AHRS and the IP Camera in a one-to-one connection set up in the Ad-Hoc mode helped evaluate their individual performance and also helped visualize the connection set up of an IEEE 802.11 wireless link. In this section, the test set up was expanded to include the W-AHRS, the IP Camera and the User Interface Node in the Ad-Hoc mode.

4.3.1. Configuring the W-AHRS and the IP Camera

The connection of multiple nodes in the Ad-Hoc mode required that the nodes be configured to operate with the same service set identifier (SSID) and a different IP Address for each node. The W-AHRS and the IP Camera were reconfigured to operate with the network name ‘2NodeAdhHoc’. Figure 4-33 shows the screenshot of the configuration page of the WiBox serial device server of the W-AHRS node. It was configured with the SSID ‘2NodeAdHoc’. The remaining network parameters are summarized in Table 12. The virtual comport settings of the W-AHRS are dependent on the IP Address of the node and hence needed no reconfiguration. Only reconfiguring the wireless settings of the WiBox was required to connect it in the Ad-Hoc mode with the user interface node.



Firmware Version: V6.5.0.0

MAC Address: 00-20-4A-96-63-DC

WLAN Settings

Wireless Network Configuration

Network Name (SSID): 2NodeAdHoc

Network Type: ○ Infrastructure ● Ad Hoc

Channel: Channel 11 United States

Wireless Network Security

Security: WEP

Authentication: Open/None

Encryption: 64 bits

Key Type: ● Hex ○ Passphrase

Key: ●●●●●●●●●●

Retype Key:

TX Key: 1

Advanced Settings

TX Data rate: 11 Mbps Auto fallback ☑

Radio Power Management: ○ Enable ● Disable

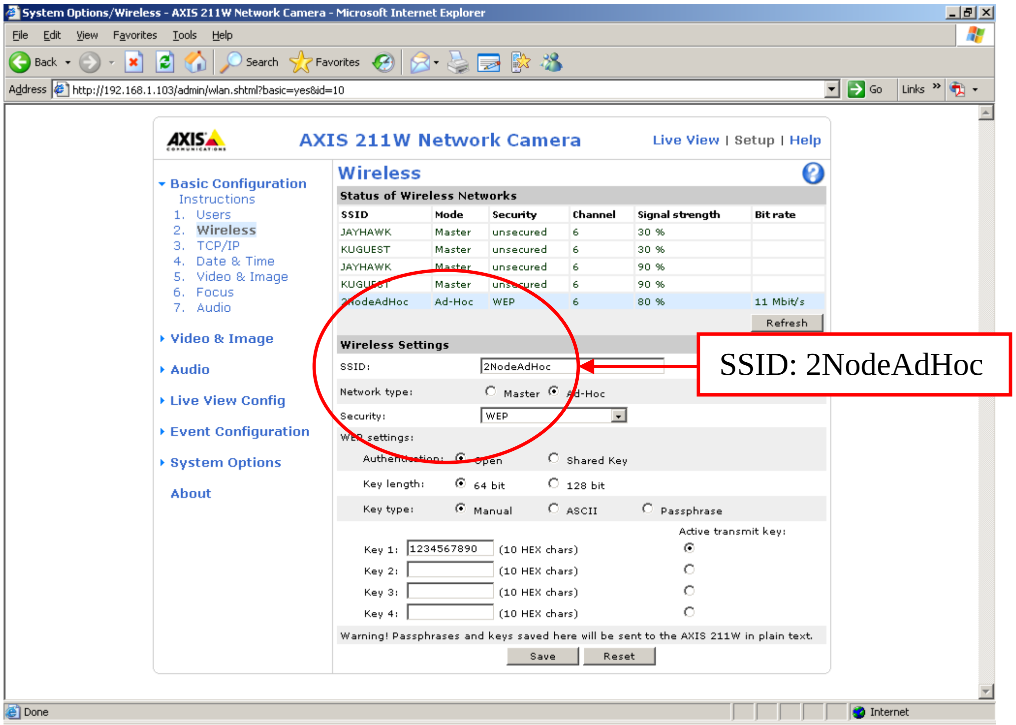
SSID: 2NodeAdHoc

Figure 4.33: Configuring the WiBox to the SSID '2NodeAdHoc'

Item	**Setting**
Topology	Ad-Hoc
Network Mode	Wireless only
Network Name (SSID)	2NodeAdHoc
IP Address	192.168.1.105
Subnet Mask	255.255.255.0
Default Gateway	None
Security suite	WEP
Authentication	Open/None
Encryption	WEP64
Encryption key	1234567890
TX Data Rate	Fixed
TX Data Rate	11 Mbps
Channel	11

Table 12: Wireless Network Settings for W-AHRS

The IP Camera was also reconfigured to operate with the same network name as the W-AHRS. Figure 4.34 shows the screenshot of the configuration page of the IP Camera. The connection settings are summarized in Table 13.



Wireless

Status of Wireless Networks

SSID	Mode	Security	Channel	Signal strength	Bit rate
JAYHAWK	Master	unsecured	6	30 %	
KUGUEST	Master	unsecured	6	30 %	
JAYHAWK	Master	unsecured	6	90 %	
KUGUEST	Master	unsecured	6	90 %	
2NodeAdHoc	Ad-Hoc	WEP	6	80 %	11 Mbit/s

Wireless Settings

SSID: 2NodeAdHoc

Network type: ○ Master ● Ad-Hoc

Security: WEP

WEP settings:

Authentication: ● Open ○ Shared Key

Key length: ● 64 bit ○ 128 bit

Key type: ● Manual ○ ASCII ○ Passphrase

Active transmit key:

Key 1: 1234567890 (10 HEX chars) ●

Key 2: (10 HEX chars) ○

Key 3: (10 HEX chars) ○

Key 4: (10 HEX chars) ○

Warning! Passphrases and keys saved here will be sent to the AXIS 211W in plain text.

SSID: 2NodeAdHoc

Figure 4.34: Configuring the IP Camera to the SSID '2NodeAdHoc'

4.35.

<table>
<tr><th colspan="2">Wireless Network Settings</th></tr>
<tr><td><b>Item</b></td><td><b>Setting</b></td></tr>
<tr><td>Wireless Network Name or SSID</td><td>2NodeAdHoc</td></tr>
<tr><td>Channel Scan</td><td>Enabled</td></tr>
<tr><td>Security Mode</td><td>WEP Enabled</td></tr>
<tr><td>Network Mode</td><td>Ad-Hoc</td></tr>
<tr><td>Network Name</td><td>ADMRCIPCAM</td></tr>
<tr><th colspan="2">Security Settings</th></tr>
<tr><td><b>Item</b></td><td><b>Setting</b></td></tr>
<tr><td>Authentication</td><td>Open</td></tr>
<tr><td>WEP Encryption</td><td>64 bit</td></tr>
<tr><td>Key Type</td><td>HEX</td></tr>
<tr><td>WEP Key 1</td><td>1234567890(needs to be 10 characters long)</td></tr>
<tr><th colspan="2">Basic TCP/IP Settings</th></tr>
<tr><td><b>Item</b></td><td><b>Setting</b></td></tr>
<tr><td>IP Address</td><td>192.168.001.105</td></tr>
<tr><td>Gateway IP Address</td><td>0.0.0.0</td></tr>
<tr><td>Subnet Mask</td><td>255.255.255.0</td></tr>
</table>

Table 13: Wireless Network Settings for IP Camera

The test setup and the network settings of the three nodes, namely the W-AHRS, the IP Camera and the User Interface Node are summarized in Figure 4.35.

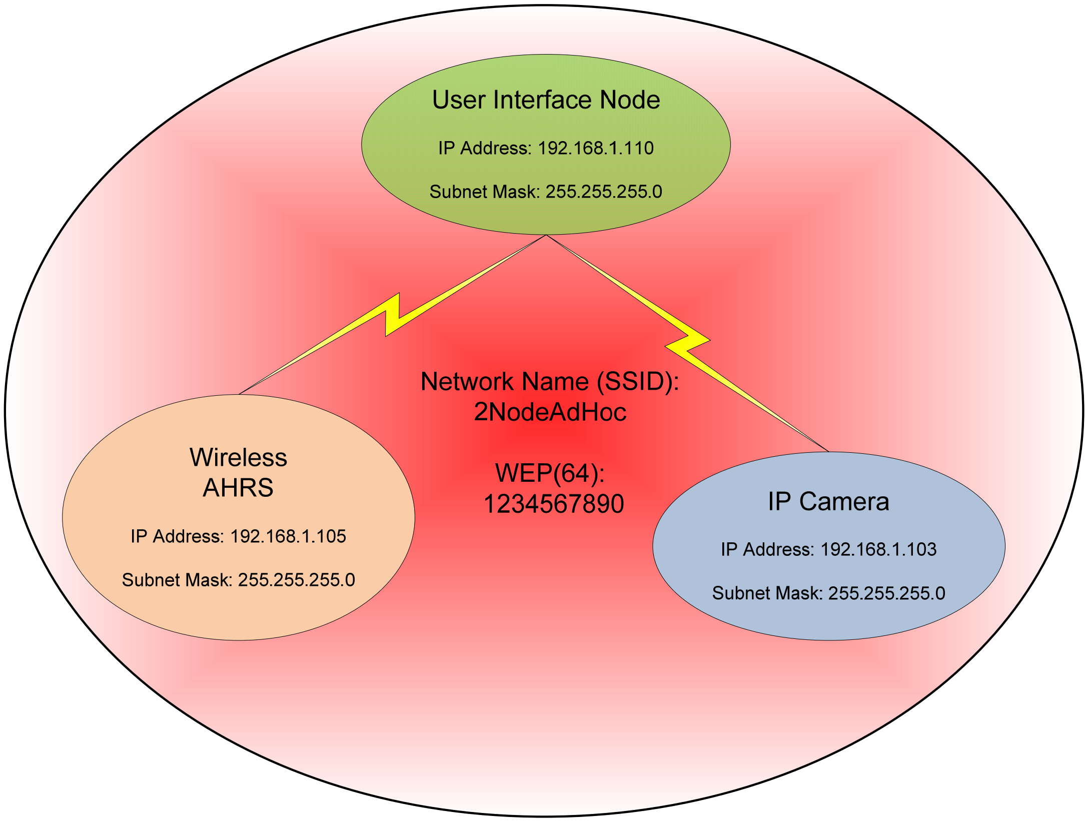
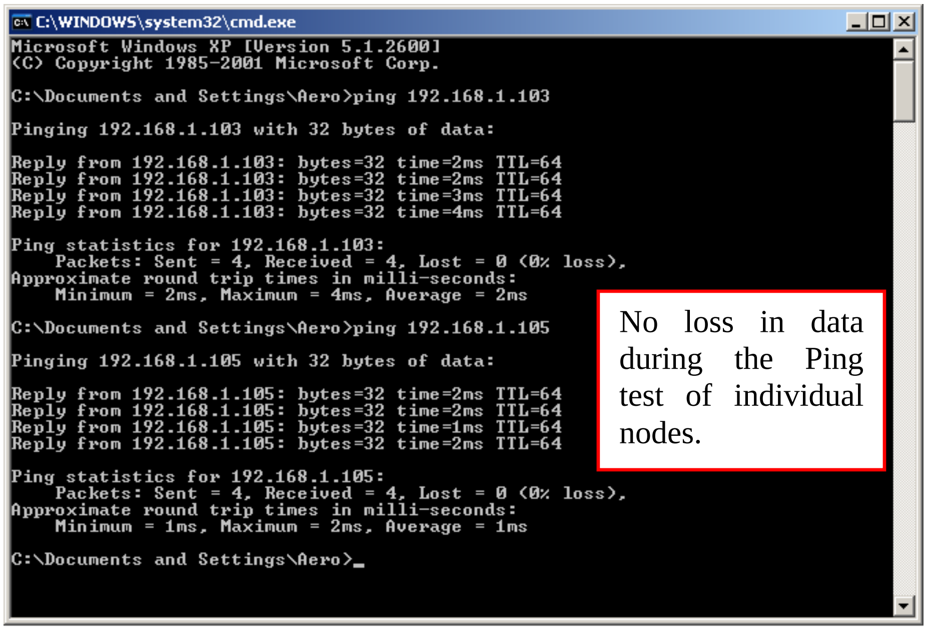

User Interface Node
IP Address: 192.168.1.110
Subnet Mask: 255.255.255.0
Network Name (SSID):
2NodeAdHoc
WEP(64):
1234567890
Wireless
AHRS
IP Address: 192.168.1.105
Subnet Mask: 255.255.255.0
IP Camera
IP Address: 192.168.1.103
Subnet Mask: 255.255.255.0

Figure 4.35: Ad-Hoc Network of Three Nodes

4.3.2. Testing of the Three Nodes in Ad-Hoc Mode

The network with the three nodes in the Ad-Hoc mode was tested to characterize the network's performance. The network was first tested using the Ping command at the command prompt. In this test, the connection of the user interface node to each node is tested on a one to one basis, that is, the connection of the user interface node to the W-AHRS node and the connection of the user interface node to the IP Camera was tested by 'pinging' them individually. Each node was tested with 4 packets of data of 32 bytes each. For the IP camera, the test showed no data loss and a maximum round trip time of 4 milliseconds. For the W-AHRS, the test showed a maximum round trip time of 2 milliseconds with 0 % loss. Figure 4.36 shows the screenshot of the 'ping' test for the two nodes.

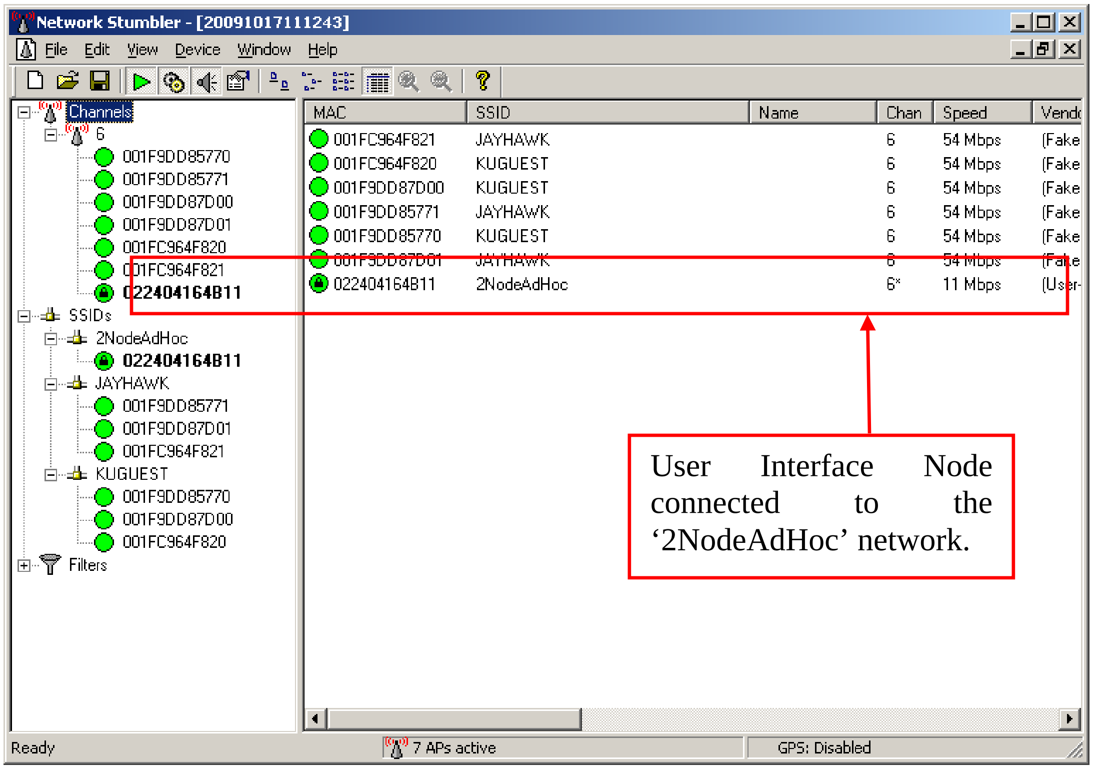


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Aero>ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:

Reply from 192.168.1.103: bytes=32 time=2ms TTL=64
Reply from 192.168.1.103: bytes=32 time=2ms TTL=64
Reply from 192.168.1.103: bytes=32 time=3ms TTL=64
Reply from 192.168.1.103: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\Aero>ping 192.168.1.105

Pinging 192.168.1.105 with 32 bytes of data:

Reply from 192.168.1.105: bytes=32 time=2ms TTL=64
Reply from 192.168.1.105: bytes=32 time=2ms TTL=64
Reply from 192.168.1.105: bytes=32 time=1ms TTL=64
Reply from 192.168.1.105: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Aero>_
```

No loss in data during the Ping test of individual nodes.

Figure 4.36: 'Ping' Test Results for the Individual Nodes

The IEEE 802.11 link of the User Interface Node, the IP Camera and the W-AHRS was then tested with Wireshark and IP Tools in the presence of multiple networks as identified by NetStumbler. Figure 4.37 shows the screen shot of NetStumber showing the presence of seven other active access points that are transmitting and are within the connecting range of the User Interface Node. It is also shown that the User Interface Node is connected to the network with the SSID ‘2NodeAdHoc’.



```
Channels
  6
    001F9DD85770
    001F9DD85771
    001F9DD87D00
    001F9DD87D01
    001FC964F820
    001FC964F821
    022404164B11
SSIDs
  2NodeAdHoc
    022404164B11
  JAYHAWK
    001F9DD85771
    001F9DD87D01
    001FC964F821
  KUGUEST
    001F9DD85770
    001F9DD87D00
    001FC964F820
Filters
```

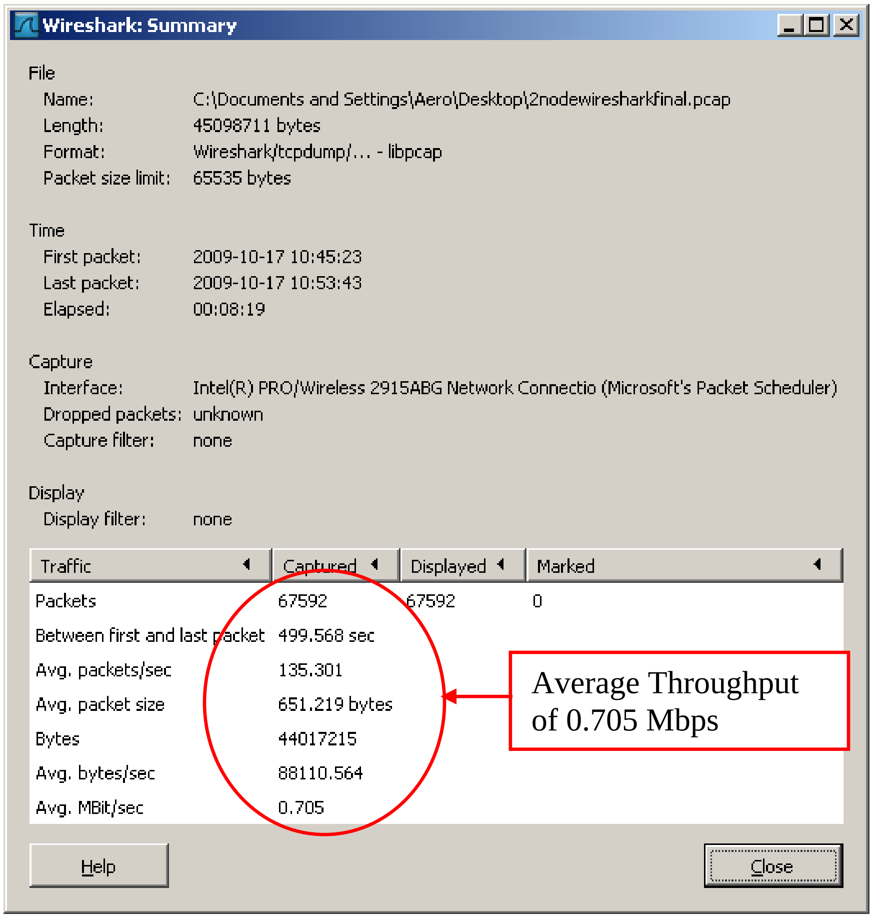
MAC	SSID	Name	Chan	Speed	Vend
001FC964F821	JAYHAWK		6	54 Mbps	(Fake
001FC964F820	KUGUEST		6	54 Mbps	(Fake
001F9DD87D00	KUGUEST		6	54 Mbps	(Fake
001F9DD85771	JAYHAWK		6	54 Mbps	(Fake
001F9DD85770	KUGUEST		6	54 Mbps	(Fake
001F9DD87D01	JAYHAWK		6	54 Mbps	(Fake
022404164B11	2NodeAdHoc		6*	11 Mbps	(User-

Ready | 7 APs active | GPS: Disabled

User Interface Node connected to the ‘2NodeAdHoc’ network.

Figure 4.37: Multiple Network Identified During The Test

The summary of the testing with Wireshark test is given in Figure 4.38. An average throughput of 0.705 Mbps was tested. The transmissions from the IP Camera were made using the User Datagram Protocol (UDP) for video transmission over the IEEE 802.11 g link and the transmission from the WiBox of the W-AHRS were made using the Transmission Control Protocol (TCP). The Parameters like Round Trip Time, Throughput and the Time Sequence Graph were measured for the transmissions using the TCP protocol.



```
File
   Name:              C:\Documents and Settings\Aero\Desktop\2nodewiresharkfinal.pcap
   Length:            45098711 bytes
   Format:            Wireshark/tcpdump/... - libpcap
   Packet size limit: 65535 bytes

Time
   First packet:      2009-10-17 10:45:23
   Last packet:       2009-10-17 10:53:43
   Elapsed:           00:08:19

Capture
   Interface:         Intel(R) PRO/Wireless 2915ABG Network Connectio (Microsoft's Packet Scheduler)
   Dropped packets:   unknown
   Capture filter:    none

Display
   Display filter:    none
```

Traffic	Captured	Displayed	Marked
Packets	67592	67592	0
Between first and last packet	499.568 sec		
Avg. packets/sec	135.301		
Avg. packet size	651.219 bytes		
Bytes	44017215		
Avg. bytes/sec	88110.564		
Avg. MBit/sec	0.705		

Average Throughput of 0.705 Mbps

Figure 4.38: Wireshark Test Summary

During the Wireshark test 67,592 packets of data were captured. These were equivalent to 44,017,215 bytes of data and were captured during a test period of 499.568 seconds. The details of the transmissions from the individual node are given in Table 14 and Table 15.

Item	**Details**
Address A (IP Camera)	**192.168.1.103**
Address B (User Interface Node)	**192.168.1.110**
Packets	**32337**
Bytes	**40286217**
Packets A→B	**32303**
Bytes A→B	**33149894**
Packets A←B	**28**
Bytes A←B	**3262**
Bits per second A→B	**636106.85**
Bits per second A←B	**63.43**
Duration	**416.85 sec**

Table 14: Connection Details for IP Camera and User Interface Node

Item	**Details**
Address A (W-AHRS)	**192.168.1.105**
Address B (User Interface Node)	**192.168.1.110**
Packets	**35234**
Bytes	**3730116**
Packets A→B	**23377**
Bytes A→B	**2570760**
Packets A←B	**9889**
Bytes A←B	**534745**
Bits per second A→B	**49338.80**
Bits per second A←B	**10265.24**
Duration	**416.85 sec**

Table 15: Connection Details for W-AHRS and the User Interface Node

An I/O graph for the connection between the two nodes and the user interface node is given in Figure 4.38. It shows that the connection was based on the User Datagram Protocol and it also shows that the connection was secure and no interference from other access points present in the vicinity affected or participated in the connection.

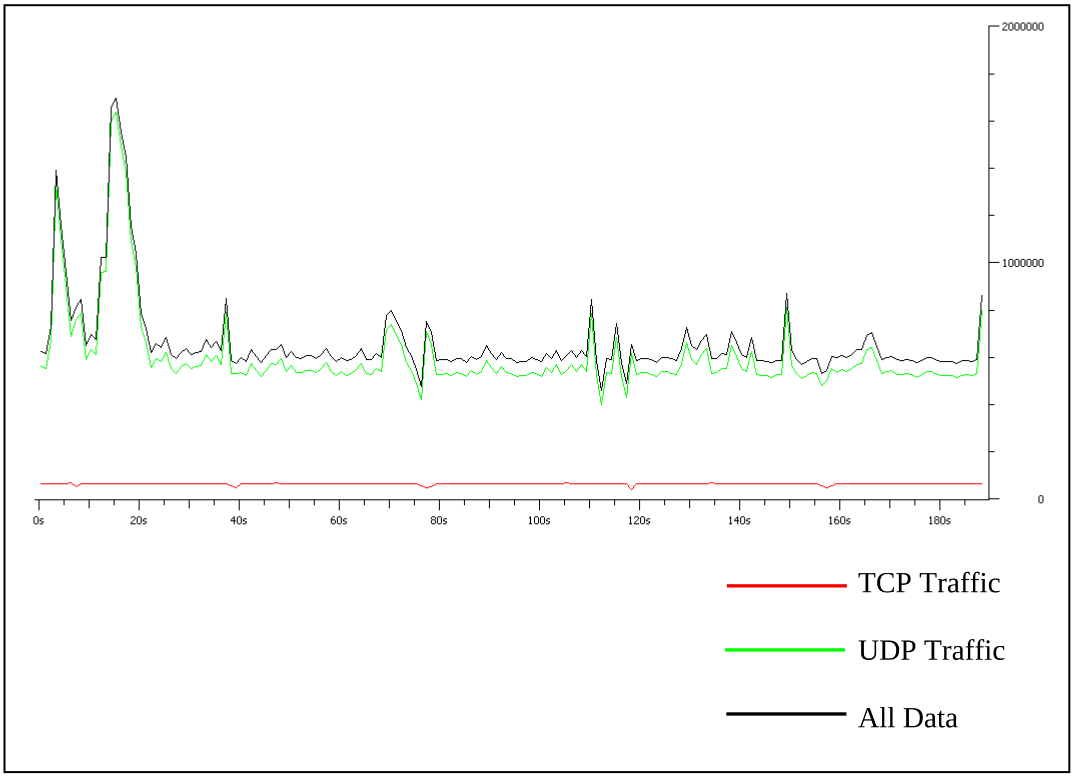


Figure 4.39: I/O Graph for the Wireshark Test

The Throughput Graph, Round Trip Time Graph and the Time Sequence Graph given in Figure 4.40 through Figure 4.42 are for the TCP traffic during the test. They are all indicative of a strong, interference free and steady connection.

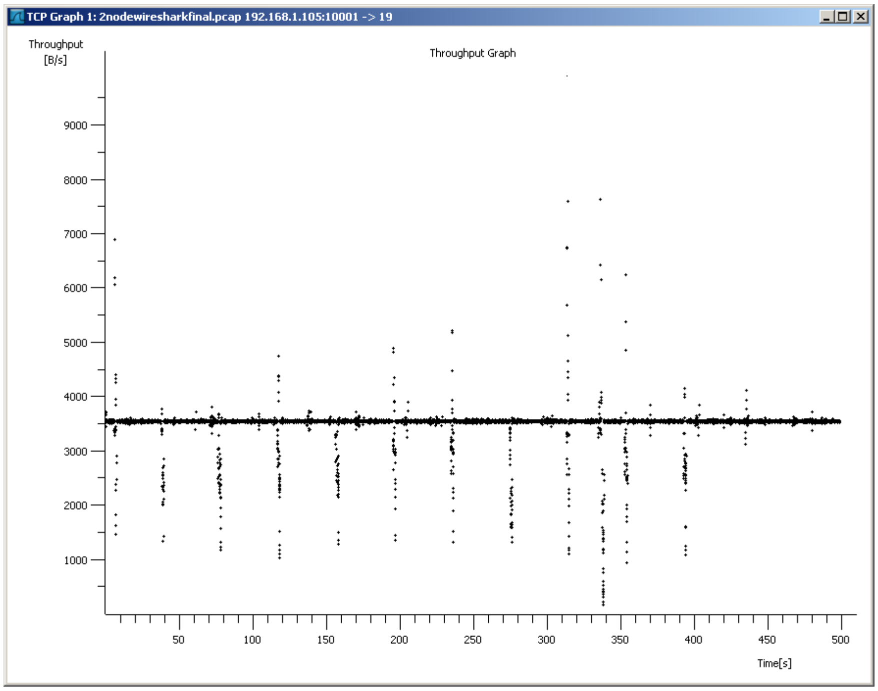


Figure 4.40: Throughput Graph for the TCP Traffic

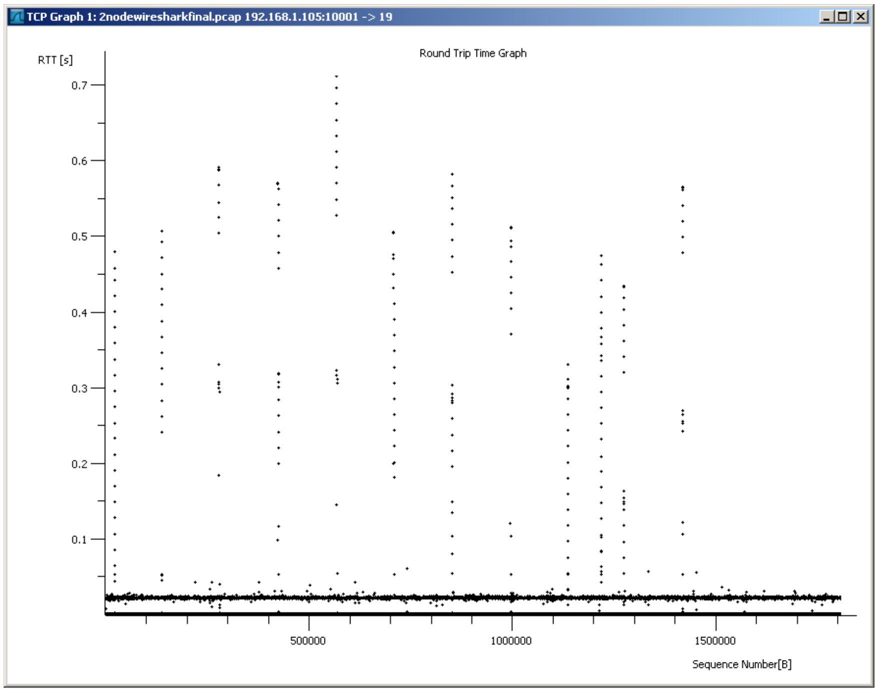


Figure 4.41: Round Trip Time Graph for the TCP Traffic

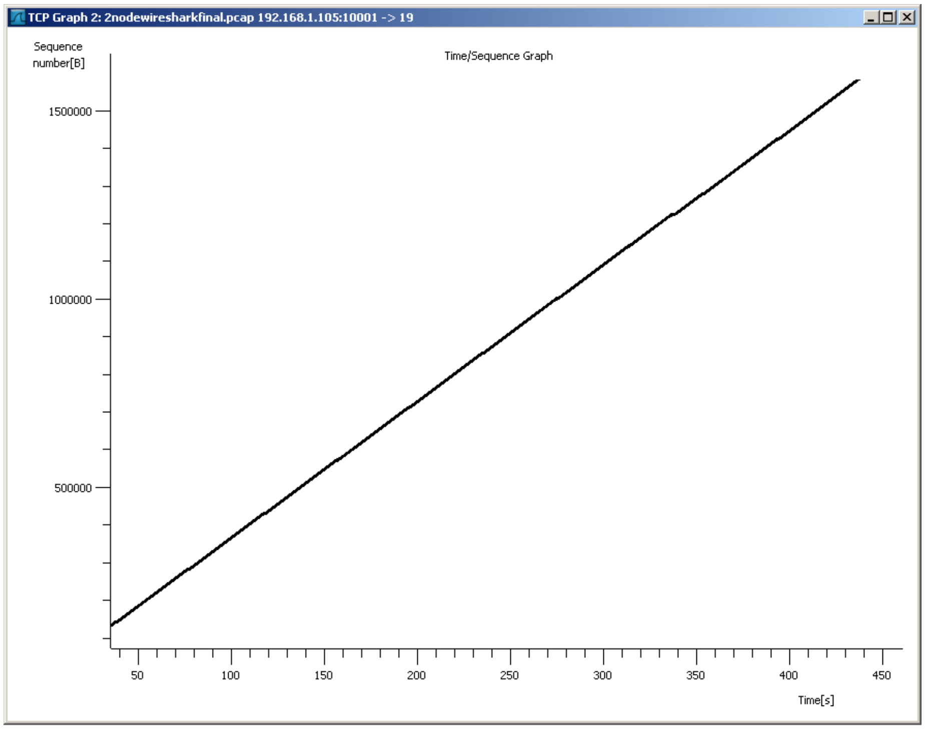


Figure 4.42: Time Sequence Graph for the TCP Traffic

The protocol distribution and analysis of the 3 node Ad-Hoc network was tested using IP Tools. The IP tools test was for a duration of 199.672 seconds during which 7,632 packets were captured.

Figure 4.43 shows that percent distribution of the two protocols during the test. In this test 52.15% of the transmissions were made using the User Datagram Protocol (UDP) and 47.85% transmissions used the Transmission Control Protocol (TCP).

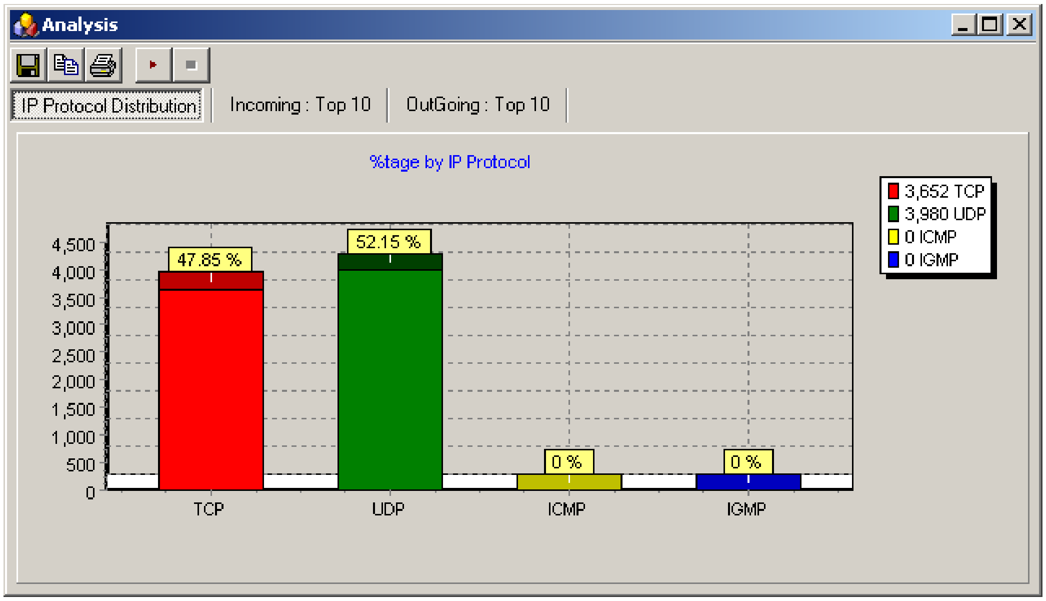


Figure 4.43: Protocol Distribution during the Testing of the 3 nodes in Ad-Hoc Mode.

Figure 4.44 shows the source IP addresses of the nodes that participated in the network. In this test 52.16% of the traffic was from the IP Camera, 31.88% of the traffic was from the W-AHRS and the remaining traffic equal to 15.96% was from the User Interface Node.

Figure 4.45 shows the destination IP addresses of the nodes that participated in the network. In this test 84.04% of the traffic was for the User Interface Node, while 15.93% of the traffic was for the W-AHRS node.

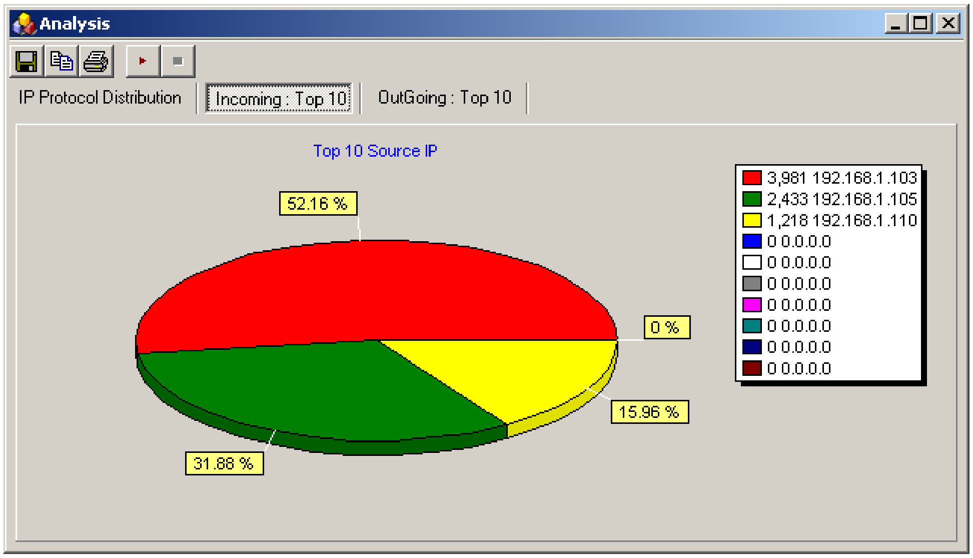


Figure 4.44: Source IP Address Distribution

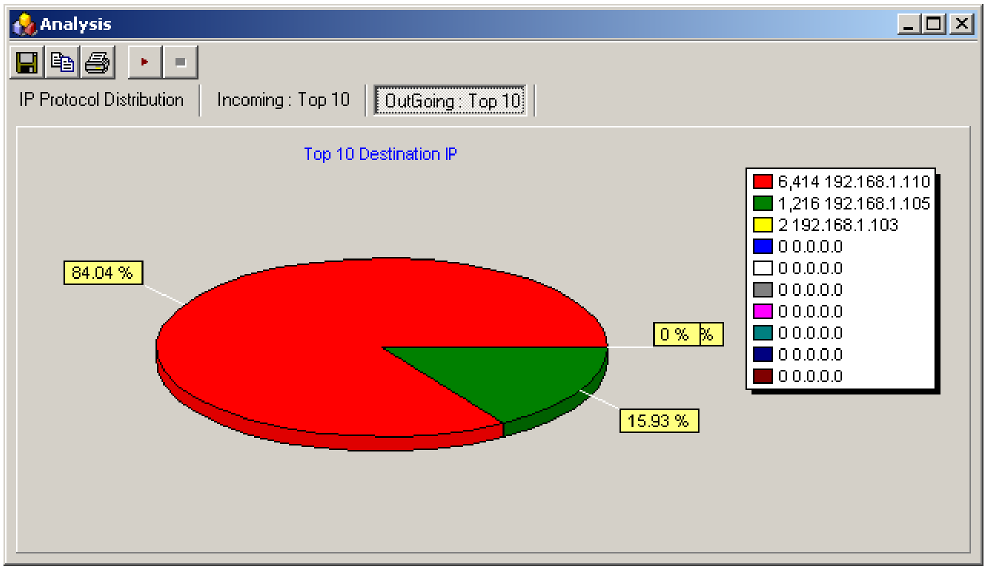


Figure 4.45: Destination IP Address Distribution

NetStumbler was also used to measure the signal-to-noise ratio of the IEEE 802.11 link between the IP Camera and the user interface node. It showed a consistently strong signal as seen in Figure 4.46.

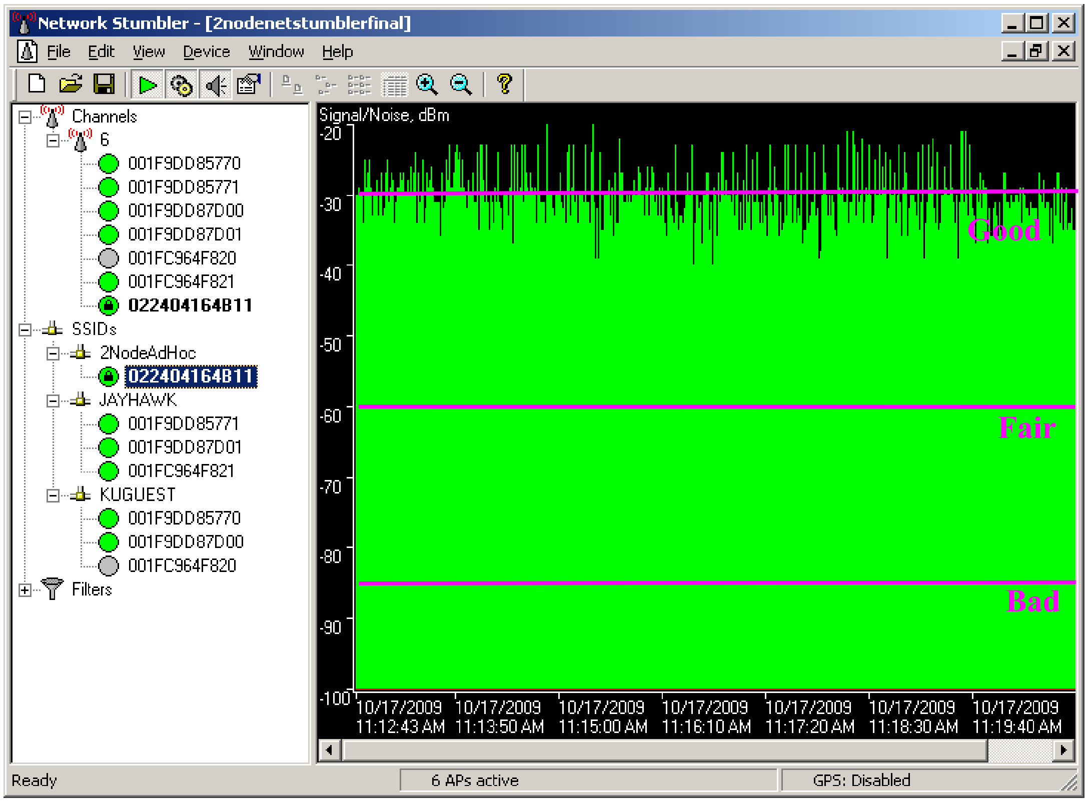


Figure 4.46: Signal To Noise Ratio Measured by NetStumbler

5. Testing in the Infrastructure Mode

An infrastructure wireless network provides for a more reliable network connection for wireless clients, since we are using a stationary base that is strategically placed for maximum reception. Also, the network operating in the infrastructure mode provides the ability to connect to a wired backbone network. The configuring of the W-AHRS and the IP Camera nodes in infrastructure mode to include an Access Point (router) and the testing of this network is described in this chapter. This represents Phase II of this project. The achieved network topology is shown in Figure 5.1.

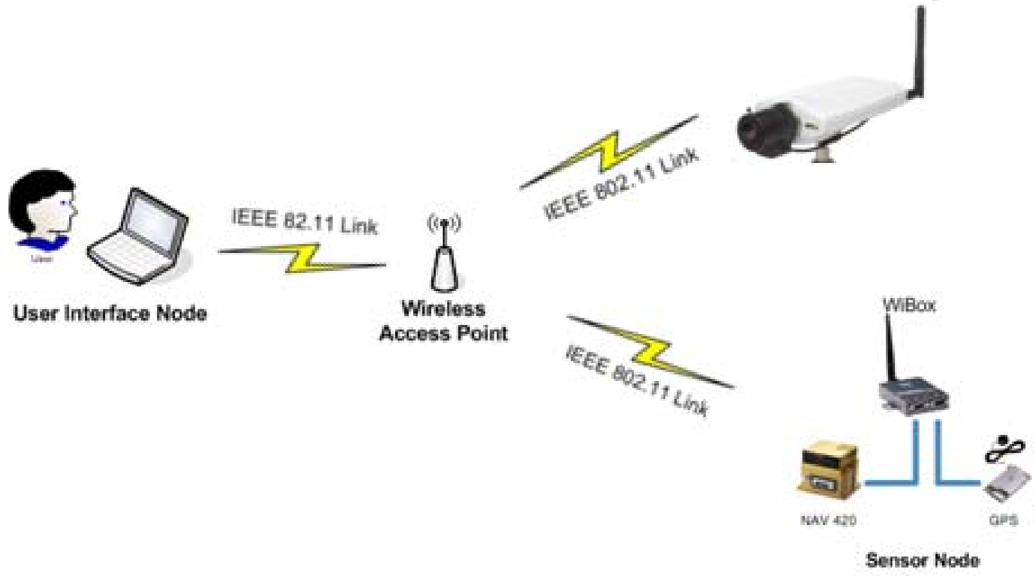


Figure 5.1: The Accomplished Network Topology in the Infrastructure Mode

5.1. Configuring the Access Point

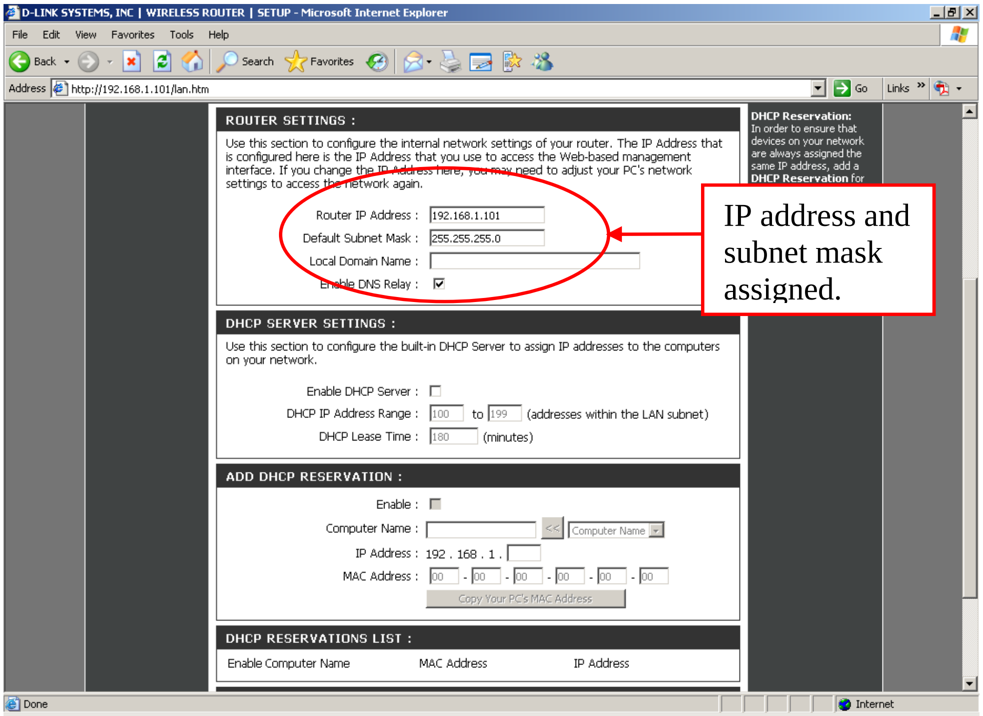
The development of a wireless network in the infrastructure mode requires the inclusion of an access point. A commercially available off-the-shelf wireless router, the D-Link® WBR 1310 Range Booster G Wireless Router was selected for inclusion in our network. The access point is show in Figures 5.1 and 5.2. This model was chosen as it permitted the use of the router for non-Internet applications, such as our project. It can be configured independently, without a pre-requisite of a DSL or cable internet connection.

Figure 5.2: D-Link® Wireless Router (Front View)

Figure 5.3: D-Link® Wireless Router (Rear View)

The Access Point (router) was configured by accessing it through a CAT 5 Ethernet Crossover Cable. The wireless router can be configured by accessing the router through a web browser on a computer. The initial IP address of the router which was 192.168.0.1 was reset to 192.168.001.101 with the subnet mask set to 255.255.255. Figure 5.3 shows a screen shot of the configuration page of the wireless router.

In the infrastructure mode, it is required that all the nodes of the network operate on the same SSID and have the same encryption standard. The SSID chosen for our network was ‘Aerohawk’. Figure 5.4 shows the configuration page of the router where the SSID and encryption are assigned to it. The configuration settings of the wireless router are summarized in Table 16.


D-LINK SYSTEMS, INC | WIRELESS ROUTER | SETUP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Copy Your PC's MAC Address
Done
Internet

http://192.168.1.101/lan.htm

ROUTER SETTINGS :

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.1.101
Default Subnet Mask : 255.255.255.0
Local Domain Name :
Enable DNS Relay : ☑

DHCP SERVER SETTINGS :

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server : □
DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)
DHCP Lease Time : 180 (minutes)

ADD DHCP RESERVATION :

Enable : □
Computer Name : << Computer Name
IP Address : 192 . 168 . 1 .
MAC Address : 00 - 00 - 00 - 00 - 00 - 00

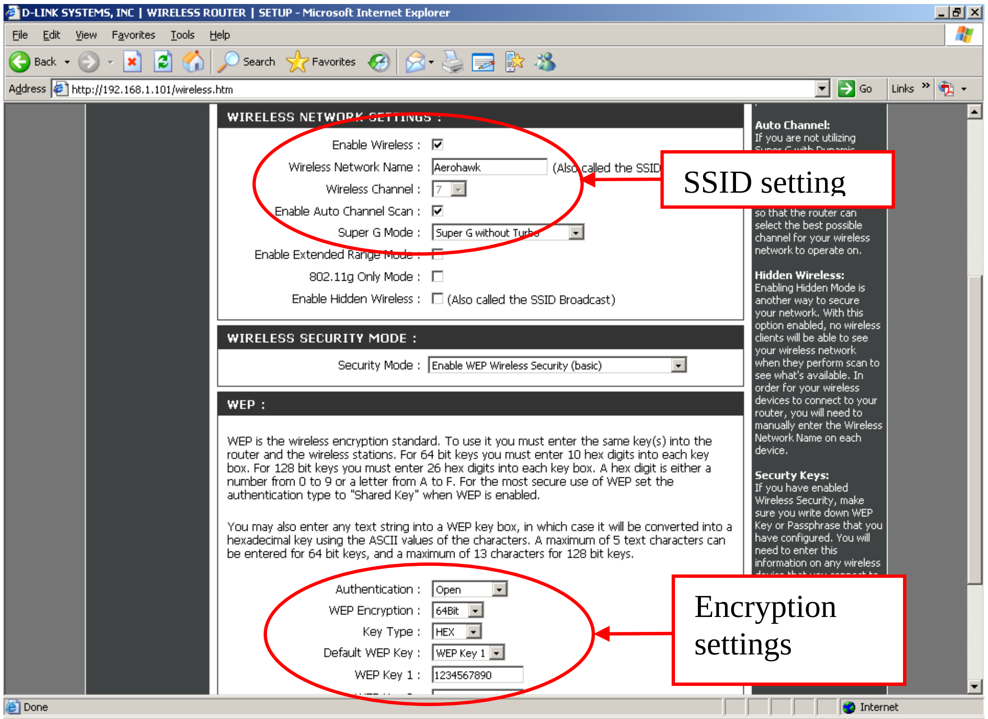
DHCP RESERVATIONS LIST :

Enable Computer Name MAC Address IP Address

DHCP Reservation:
In order to ensure that devices on your network are always assigned the same IP address, add a DHCP Reservation for

IP address and subnet mask assigned.

Figure 5.4: Configuring the Wireless Router


D-LINK SYSTEMS, INC | WIRELESS ROUTER | SETUP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.101/wireless.htm
Go Links
SSID setting
Encryption settings
Done
Internet

WIRELESS NETWORK SETTINGS :

Enable Wireless : ☑

Wireless Network Name : Aerohawk (Also called the SSID

Wireless Channel : 7

Enable Auto Channel Scan : ☑

Super G Mode : Super G without Turbo

Enable Extended Range Mode : □

802.11g Only Mode : □

Enable Hidden Wireless : □ (Also called the SSID Broadcast)

WIRELESS SECURITY MODE :

Security Mode : Enable WEP Wireless Security (basic)

WEP :

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

Authentication : Open

WEP Encryption : 64Bit

Key Type : HEX

Default WEP Key : WEP Key 1

WEP Key 1 : 1234567890

Auto Channel:
If you are not utilizing

so that the router can select the best possible channel for your wireless network to operate on.

Hidden Wireless:
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

Securty Keys:
If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless

Figure 5.5: Configuring the Wireless Router (contd.)

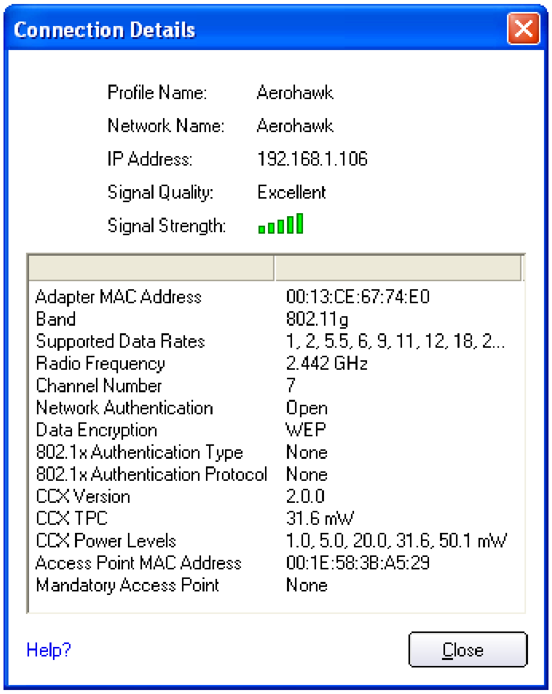
Wireless Network Settings	
Item	**Setting**
Wireless Network Name (SSID)	Aerohawk
Channel Scan	Enabled
Security Mode	WEP Enabled
IP Address	192.168.1.101
Subnet Mask	255.255.255.0
Security Settings	
Authentication	Open
WEP Encryption	64 bit
Key Type	HEX
WEP Key 1	1234567890 (needs to be 10 characters long)

Table 16: Network and Security Settings of the Wireless Router

5.2. Configuring the Nodes to the Access Point

The inclusion of the Access Point into the network was completed by reconfiguring the individual nodes i.e., the W-AHRS, the IP Camera and the User Interface Node, to communicate with the access point in the infrastructure mode and not with each other as in the Ad-Hoc mode. The configuration of the User Interface Node, IP Camera and the W-AHRS is presented in this section.

The User Interface Node (the laptop computer) was configured to connect to the access point. The result of the configuration and the successful connection of the User Interface Node to the Access Point is shown in Figure 5.5.



Profile Name: Aerohawk
Network Name: Aerohawk
IP Address: 192.168.1.106
Signal Quality: Excellent
Signal Strength:

Adapter MAC Address	00:13:CE:67:74:E0
Band	802.11g
Supported Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 2...
Radio Frequency	2.442 GHz
Channel Number	7
Network Authentication	Open
Data Encryption	WEP
802.1x Authentication Type	None
802.1x Authentication Protocol	None
CCX Version	2.0.0
CCX TPC	31.6 mW
CCX Power Levels	1.0, 5.0, 20.0, 31.6, 50.1 mW
Access Point MAC Address	00:1E:58:3B:A5:29
Mandatory Access Point	None

Figure 5.6: Successful Connection of the User Interface Node to the Access Point

The User Interface Node was connected to the Access Point by configuring it with the same security settings and WEP key as used in the access point.

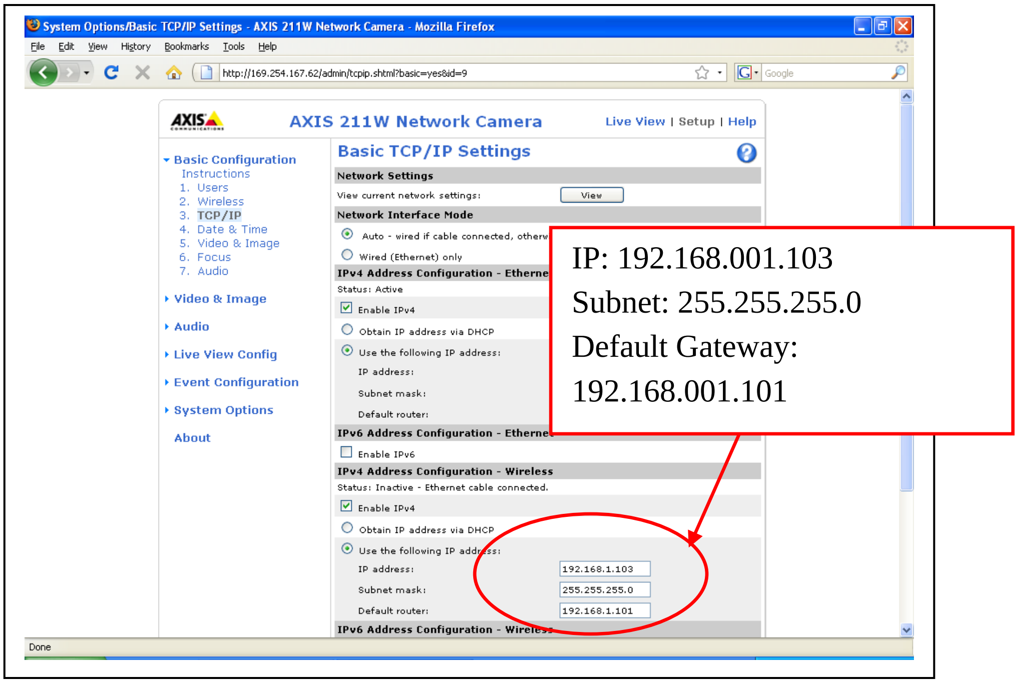
The wireless AHRS was reconfigured to connect to the Access Point. For this, the Wi-Fi based serial device server of the W-AHRS node was accessed through HyperTerminal and a new set of IP addresses, with a new SSID and WEP key were assigned to it. The WiBbox serial device server was assigned the IP address 192.168.001.105. Table 17 shows the summary of the configuration changes done to the WiBox serial device server to enable it to connect to the Access Point.

Wireless Network Settings	
Item	**Setting**
IP Address	192.168.001.105
Gateway IP Address	192.168.001.101
Network Mode	Infrastructure
Network Name	Aerohawk
Authentication	Open
Encryption	WEP64
Key Type	HEX
WEP Key	1234567890

Table 17: Wireless and Security Settings of the WiBox of AHRS Node

The video node which was initially configured in the Ad-Hoc mode was also reconfigured to the same settings of the access point to include it in the network. These settings are shown in Figure 5.6.

With the following reconfiguration of the individual nodes, the network was designed to communicate in the infrastructure mode with the access point providing connectivity to the user interface node.



Basic TCP/IP Settings

Network Settings

View current network settings:

Network Interface Mode

● Auto - wired if cable connected, otherw

○ Wired (Ethernet) only

IPv4 Address Configuration - Etherne

Status: Active

☑ Enable IPv4

○ Obtain IP address via DHCP

● Use the following IP address:

IP address:

Subnet mask:

Default router:

IPv6 Address Configuration - Etherne

☐ Enable IPv6

IPv4 Address Configuration - Wireless

Status: Inactive - Ethernet cable connected.

☑ Enable IPv4

○ Obtain IP address via DHCP

● Use the following IP address:

IP address: 192.168.1.103

Subnet mask: 255.255.255.0

Default router: 192.168.1.101

IPv6 Address Configuration - Wireless

IP: 192.168.001.103
Subnet: 255.255.255.0
Default Gateway:
192.168.001.101

Figure 5.7: Reconfiguring the Video Node

5.3. Ground Testing the Network

The network with both the sensor nodes configured to communicate with the Access Point and thus providing continuous data to the user interface node was ground tested on a moving platform - a car. The power required for operating the camera and the Access Point was obtained from a 12 V, 7 Amp-hr battery. The battery made the Access Point and the IP Camera as stand alone units and powers the devices for about one hour. For future flight testing, they would not require any power from the airplane. The devices can be installed directly with little or no modification to the test plane. Figure 5.8 shows the IP Camera and the Access Point connected to the battery through a regulator.

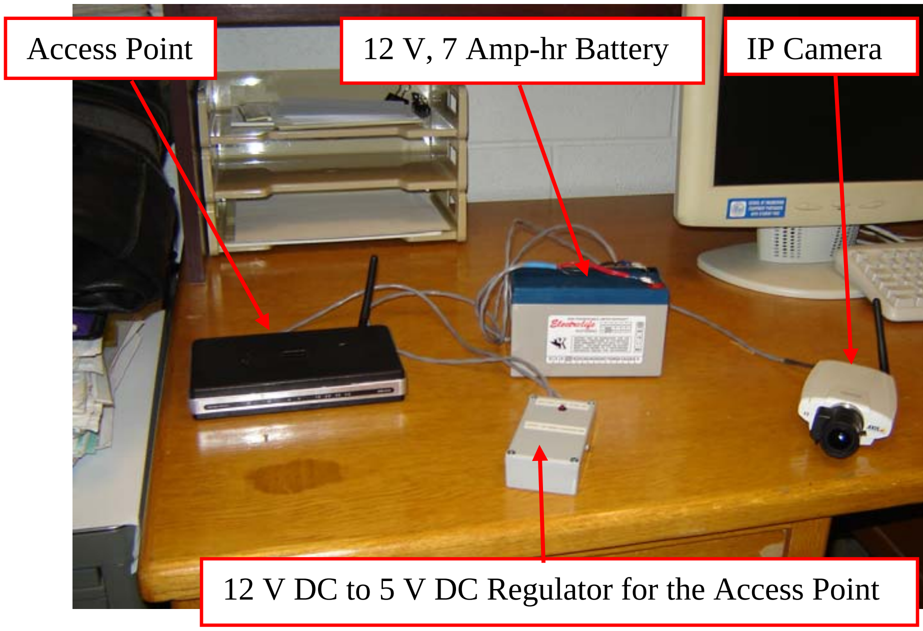


Figure 5.8: A 12V, 7Amp Battery Powered the IP Camera and Access Point

The ground testing of the network on a mobile platform was conducted in two modes. In the first test scenario, the two node wireless network along with the Access Point was set up in the car and the User Interface Node was held outside at a fixed distance of about 75 ft. The car was made to go around the engineer operating the user interface node over a constant radius of about 75 ft. The engineer operating the User Interface Node was responsible for data logging and testing the performance of the network. The test was conducted for about 15 minutes with data logged for about 5 minutes. Figures 5.9 through 5.12 show the test set up for this test.

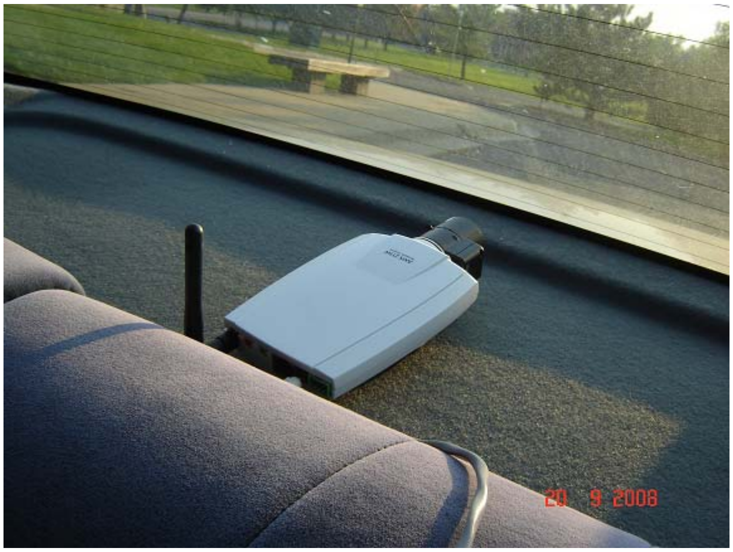


Figure 5.9: IP Camera in the Rear of the Car

Figure 5.10: Power Cable for the IP Camera

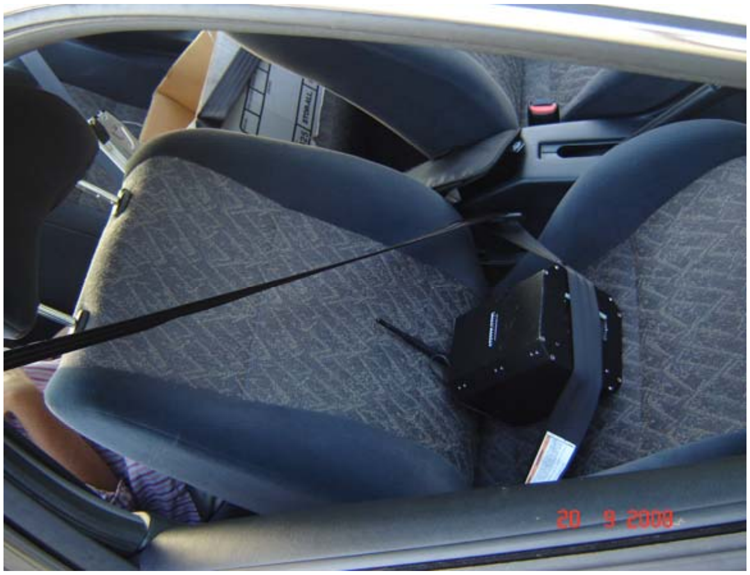


Figure 5.11: The W-AHRS Unit in the Front Seat

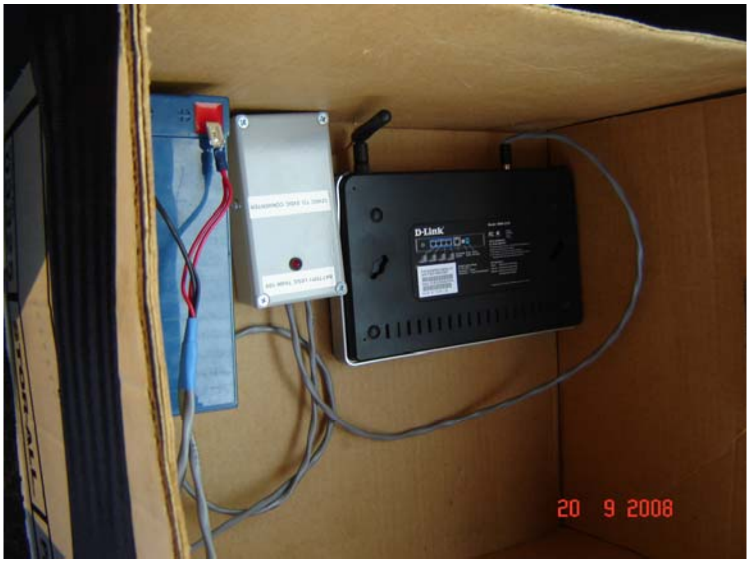


Figure 5.12: The Access Point and the Battery

For the second mode of testing the network in the car, the engineer operating the user interface node was seated in the rear seat. The car was driven around the university's campus for about 15 minutes and the performance of the network was evaluated. This test validated the network's reliability and performance for a flight test. Figure 5.13 shows the engineer seated in the back seat of the car and operating the User Interface Node. The box containing the access point and the battery can be seen beside him.

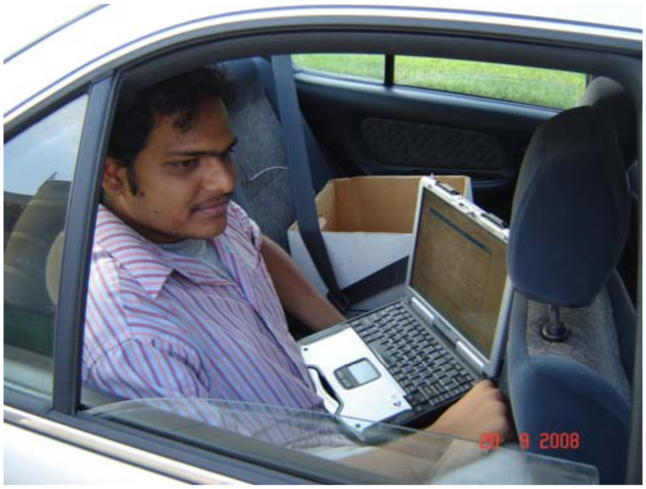
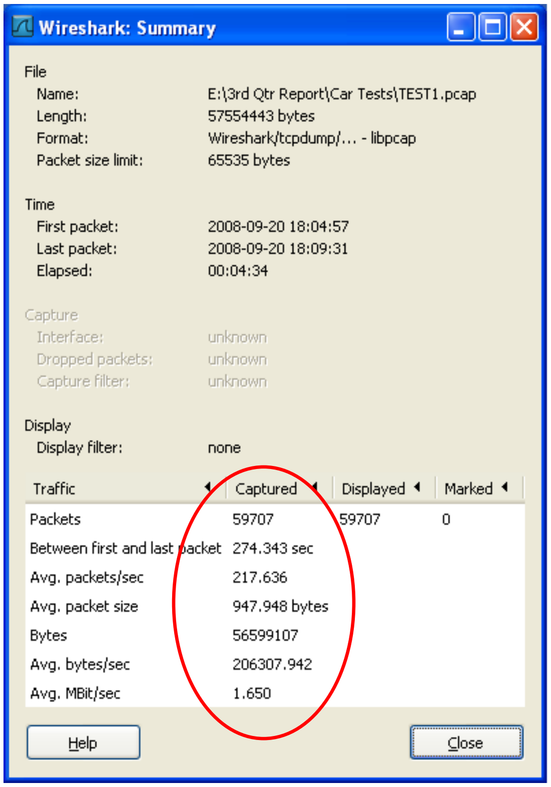

20 9 2008

Figure 5.13: Engineer in the Back Seat of Vehicle

The results from the two modes of testing of the network are presented below. The network performed flawlessly. There was no interference from other networks and access points present in the vicinity. The video streaming from the IP Camera was captured and stored on the User Interface Node. Snapshots taken by the IP Camera during the recording and testing were also stored on the User Interface Node. The wireless AHRS unit was accessible continuously throughout the test period, showing real time navigation on the NAV-VIEW software running on the User Interface Node. The link between the user interface node and the access point was 'excellent' throughout the test periods.

Figure 5.14 shows the Wireshark summary of the test when the User Interface Node was outside the vehicle. The Wireshark test was for a duration of 274.343 seconds during which 59,707 packet of data, equivalent to 565,991,107 bytes, were captured.



Wireshark: Summary

File
Name: E:\3rd Qtr Report\Car Tests\TEST1.pcap
Length: 57554443 bytes
Format: Wireshark/tcpdump/... - libpcap
Packet size limit: 65535 bytes

Time
First packet: 2008-09-20 18:04:57
Last packet: 2008-09-20 18:09:31
Elapsed: 00:04:34

Capture
Interface: unknown
Dropped packets: unknown
Capture filter: unknown

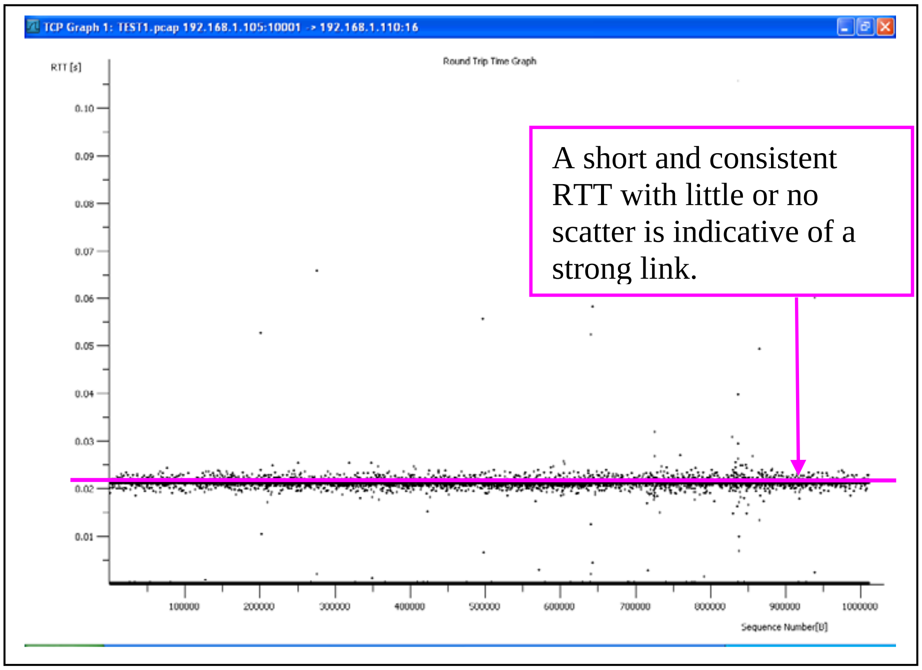
Display
Display filter: none

Traffic	Captured	Displayed	Marked
Packets	59707	59707	0
Between first and last packet	274.343 sec		
Avg. packets/sec	217.636		
Avg. packet size	947.948 bytes		
Bytes	56599107		
Avg. bytes/sec	206307.942		
Avg. MBit/sec	1.650		

Figure 5.14: Summary of Ground Testing – Mode 1

Mode 1 – User Interface Node Outside the Vehicle

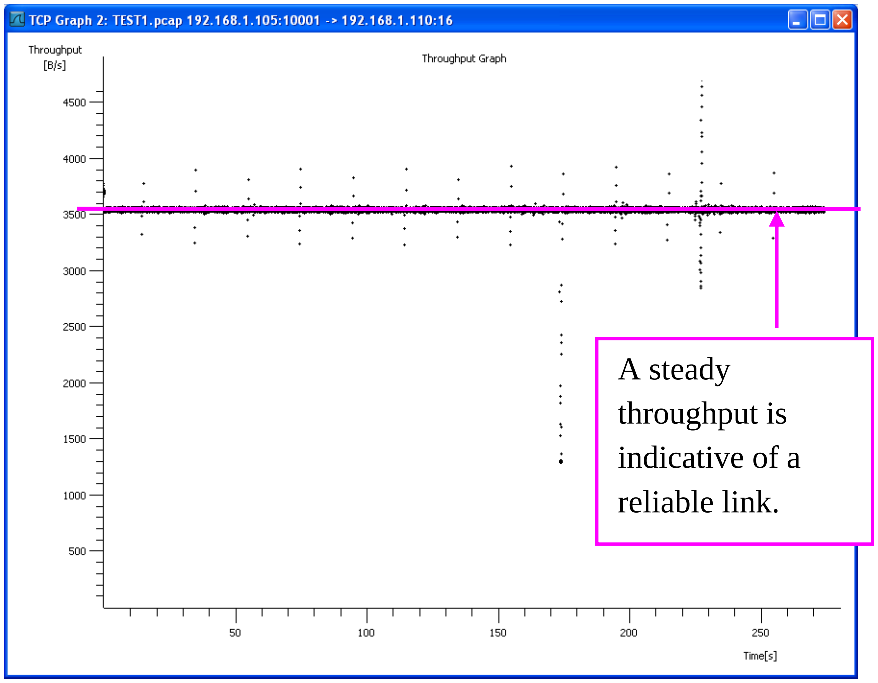
The Round Trip Time Graph for the test is given in Figure 5.15. A mean round trip time of 0.02 sec was observed. It is indicative of a congestion free connection that is not affected by the other networks. The Throughput Graph for the test, shown in Figure 5.16, also indicates a reliable communication link with a steady performance.



A short and consistent RTT with little or no scatter is indicative of a strong link.

Figure 5.15: Round Trip Time Graph for Mode 1

Mode 1 - User Interface Node Outside the Vehicle

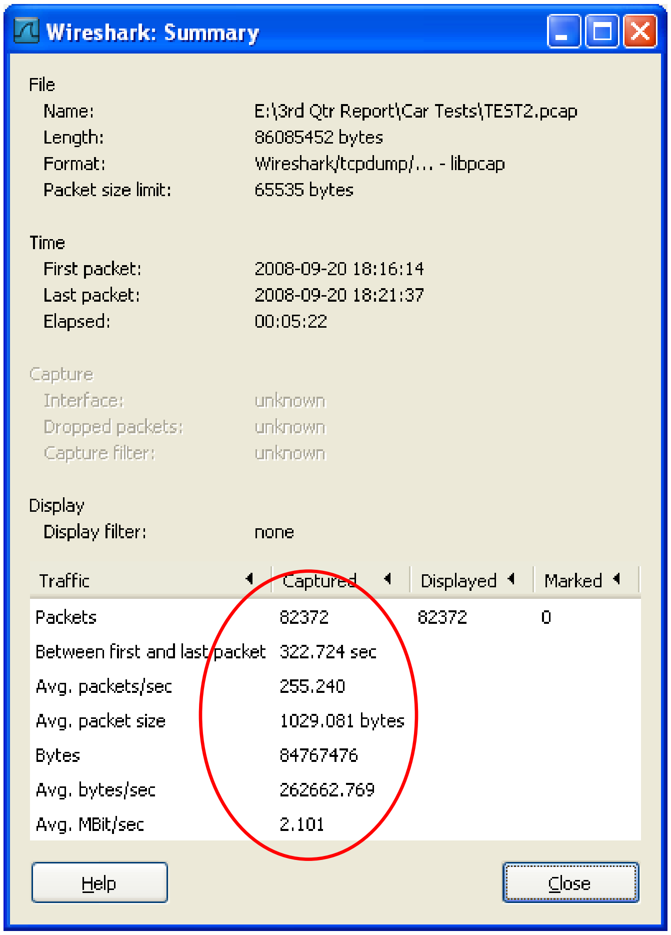


A steady throughput is indicative of a reliable link.

Figure 5.16: Throughput Graph for Mode 1

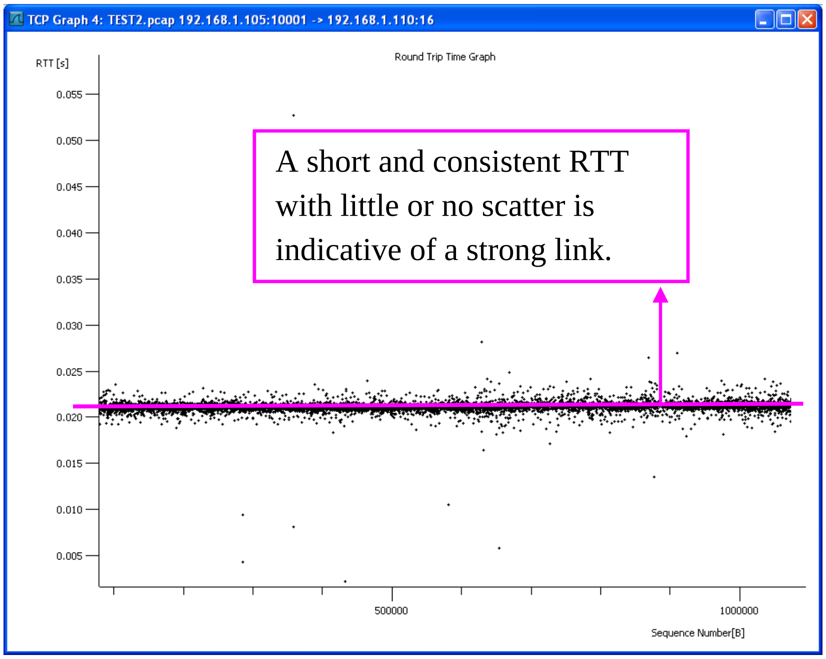
A steady round trip time and a consistent throughput are indicative of a connection that is not affected by surrounding networks due to congestion, re-transmission and duplicate acknowledgements.

Figure 5.17 shows the summary of the Wireshark test for Mode 2, in which the vehicle was moving continuously and the User Interface Node was operated inside the vehicle. This test was for a duration of 322.27 sec, during which 82,372 packets of data equivalent to 84,767,476 bytes were captured.



```
File
  Name:                 E:\3rd Qtr Report\Car Tests\TEST2.pcap
  Length:               86085452 bytes
  Format:               Wireshark/tcpdump/... - libpcap
  Packet size limit:    65535 bytes

Time
  First packet:         2008-09-20 18:16:14
  Last packet:          2008-09-20 18:21:37
  Elapsed:              00:05:22

Capture
  Interface:            unknown
  Dropped packets:      unknown
  Capture filter:       unknown

Display
  Display filter:       none

 Traffic                        Captured        Displayed    Marked
Packets                         82372           82372        0
Between first and last packet   322.724 sec
Avg. packets/sec                255.240
Avg. packet size                1029.081 bytes
Bytes                           84767476
Avg. bytes/sec                  262662.769
Avg. MBit/sec                   2.101
```

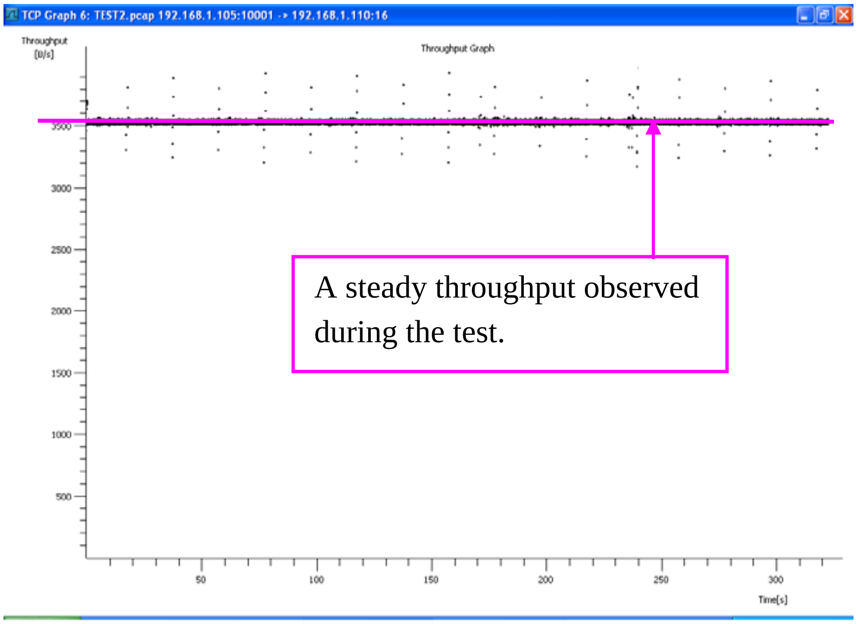
Figure 5.17: Summary of Ground Testing – Mode 2



A short and consistent RTT with little or no scatter is indicative of a strong link.

Figure 5.18: Round Trip Time Graph for Mode 2

Mode 2 – User Interface Node Inside the Vehicle



A steady throughput observed during the test.

Figure 5.19: Throughput Graph for Mode 2

The Round Trip Time Graph for the test is given in Figure 5.18. A mean round trip time of 0.022 sec was observed. It is indicative of a congestion free connection that is not affected by the other networks. The Throughput Graph for the test, shown in Figure 5.19, also indicates a reliable communication link with a steady performance. A steady round trip time and a consistent throughput are indicative of a connection that is not affected by surrounding networks due to congestion, re-transmission and duplicate acknowledgements. A snapshot taken by the IP Camera during the test is given in Figure 5.20.

Figure 5.20: Snapshot from IP Camera, Mode 1 Testing

5.4. Flight Test

The results from the ground testing of the network in a moving vehicle established that the network was reliable and interference free. The successful ground testing was the basis for proceeding to flight testing of the network in a Cessna 172 to establish the viability of the IEEE 802.11 protocol for avionics application.

The flight test of the network consisting of the User Interface Node, the Wireless AHRS unit, the IP Camera and the Access Point was conducted in a Cessna 172. The installation of the network was completed with no modification to the aircraft. The nodes of the network were powered by two 12 V batteries that were installed in the aircraft at safe and viable locations. The battery that was used to power the W-AHRS node was included in the container, making it a fully operational and self sufficient node. The battery used to power the IP Camera and the Access Point was installed at the base of one of the seats in the aircraft.

The wireless Attitude Heading Reference System was installed on the aircraft by tying it down in the luggage bay of the aircraft. Tie down points were made on the container housing the W-AHRS using metal wire. These points were used to securely tie the node to the aircraft using the tie down points available in the aircraft. The battery used to power the IP Camera and the Access Point was securely tied to the base of the rear seat of the aircraft. It was tied using tie down points that were made by using plastic rope and zip ties. The location to tie down the battery was chosen so that it was possible for the test engineer to easily unplug the wires, if required, during the flight test.

The Access Point and the IP Camera were placed in the pouch at the back of the pilot's seat during take-off and landing. During the test, the IP Camera was held and operated by the test engineer in the front seat, beside the pilot. All the arrangements were inspected thoroughly on the day of the test by the flight test engineer and the pilot-in-command. The advantages to employing wireless sensors were evident in the ease of setting up the network for the flight test. The aircraft needed no structural modification that would have necessitated extensive documentation and evaluation of the test set up. Also, the inclusion of the batteries to power the sensors obviated any modification to the electrical systems. The pilot-in-command was consulted extensively on the installation of the equipment and the test was conducted only after his inspection and approval of the test set up. The details of the flight test along with the associated documentation are included in Appendix A.

The flight test was done over a typical flight regime consisting of the following maneuvers: Rate 1 Turns, Steep Turns, Elevator/Aileron/Rudder Short Impulses and Doublets, Sideslips, Slow Flight, Acceleration and Elevator/Aileron/Rudder Frequency Sweeps. The network was tested using

Wireshark and IP Tools during the flight test. Data was logged during each maneuver using the NAV-VIEW software installed on the User Interface Node.

The system performance was measured and there were no instances of the network failing. The COMM check and the NAV Check performed by the pilot-in-command before take-off ensured that there was no EMI affecting the performance of the onboard electronic flight instrumentation. The flight test procedure consisted of data logging for each maneuver. The pilot-in-command indicated the start and stop for each maneuver so that the test engineer could log data in independent files for post flight test processing. The pilot-in-command had no complains of the wireless network affecting the onboard instrumentation at any point during the flight test.

The post flight test processing of the data from the test indicated that the wireless network provided a reliable means of data transmission for avionics application. During the test no discrepancies were observed in the communication links from the nodes to the User Interface Node. Sample results from the data logging from the W-AHRS sensor node are given in Figures 5.23 through 5.27. The unfiltered data has been plotted in MATLAB and the maneuvers are shown in overlay using Google Earth screenshots. The screenshots show that the data logging was continuous with no blocks of missing data. The Google Earth screenshots and plots for all the maneuvers are given in Appendix B.

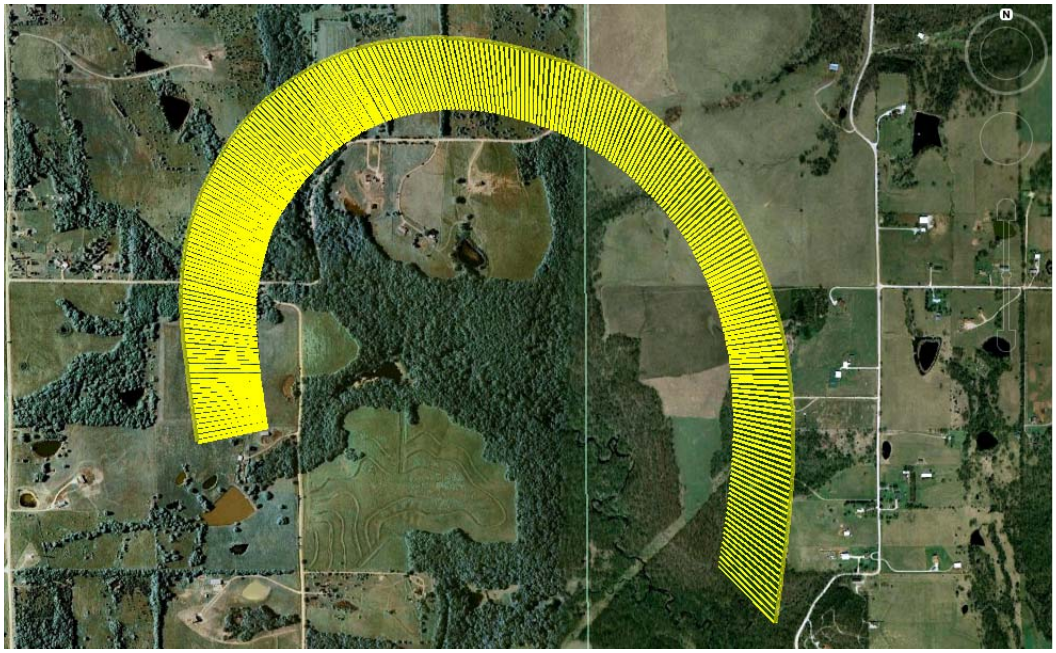


Figure 5.21: Google Earth Screenshot of Rate 1 Turn (Left)

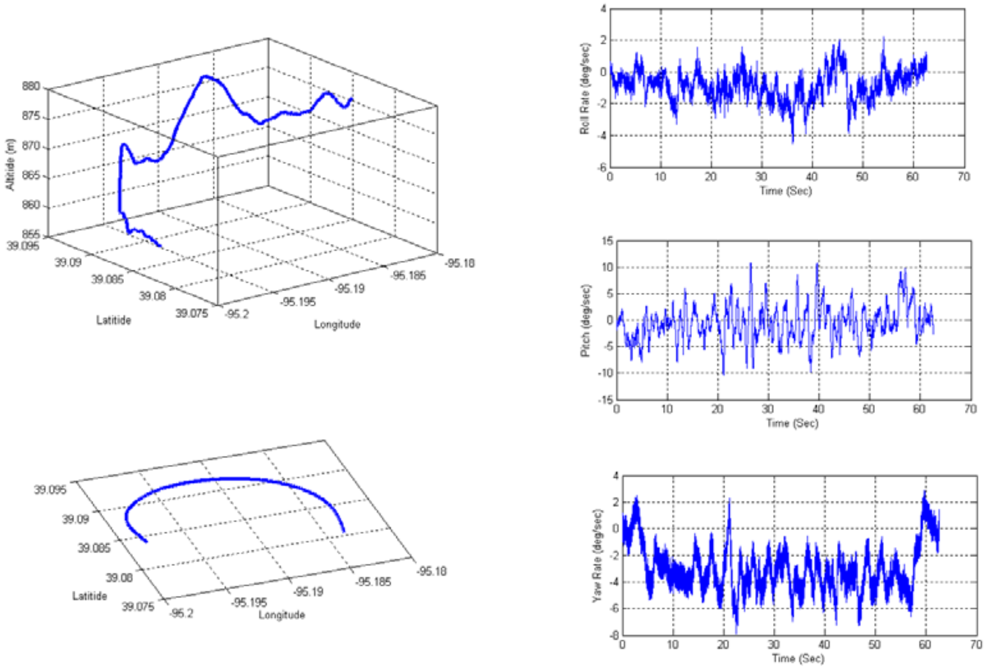


Figure 5.22: MATLAB plot of Rate 1 Turn (Left)

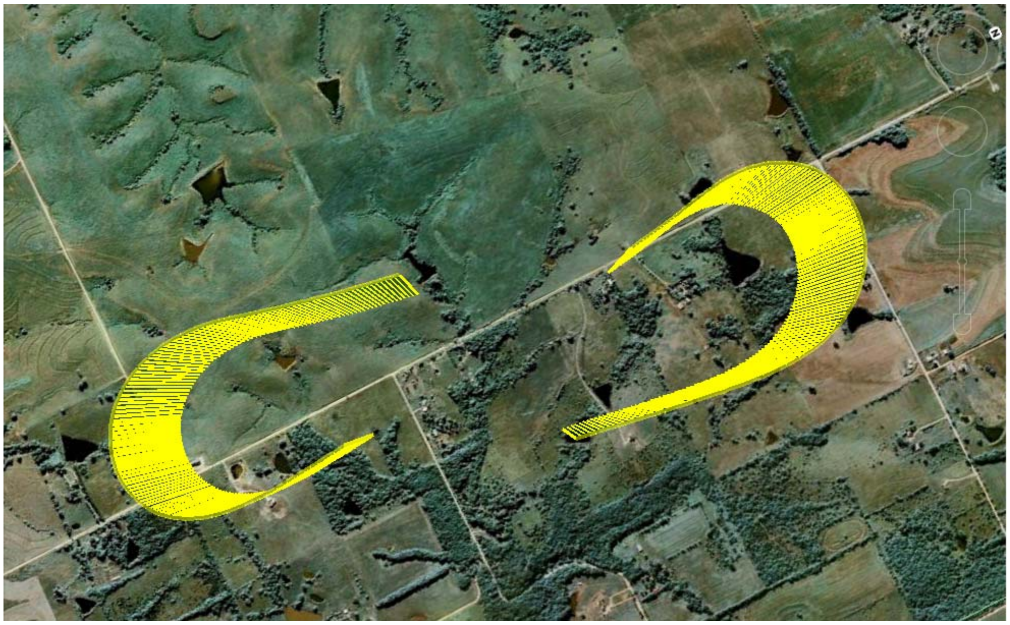


Figure 5.23: Google Earth Screen Shot of the Steep Turn Maneuvers

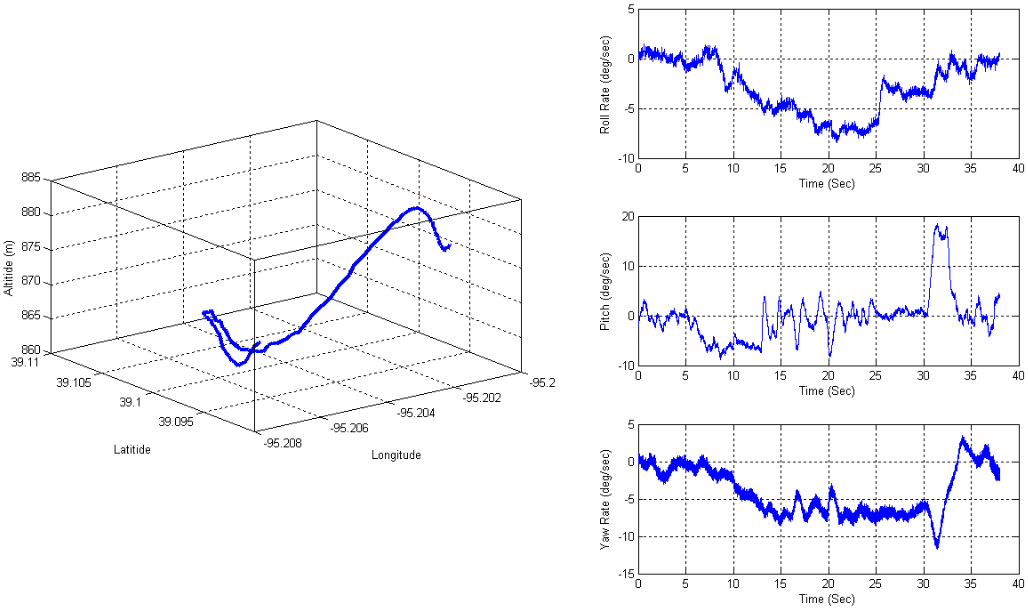


Figure 5.24: MATLAB Plot of Left Steep Turn Maneuver

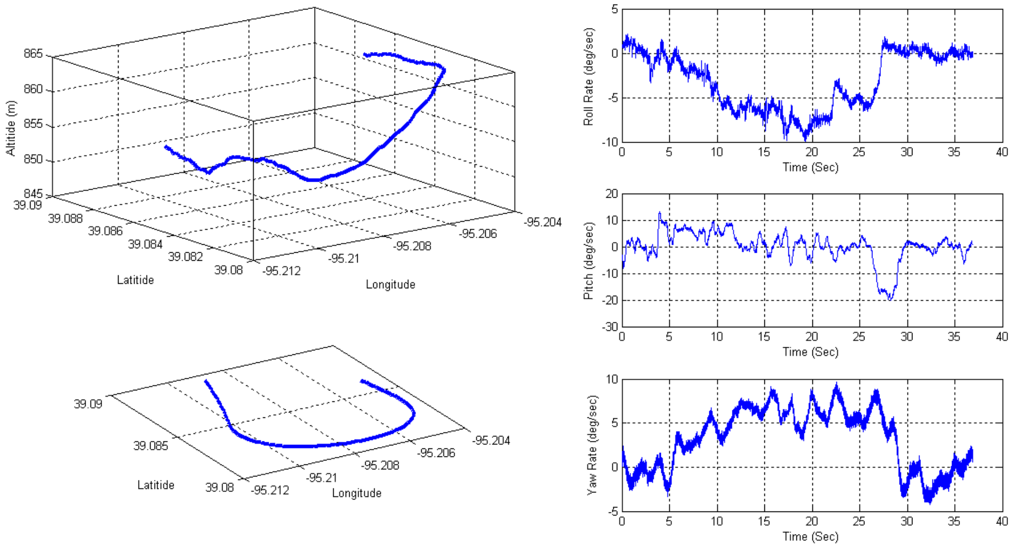
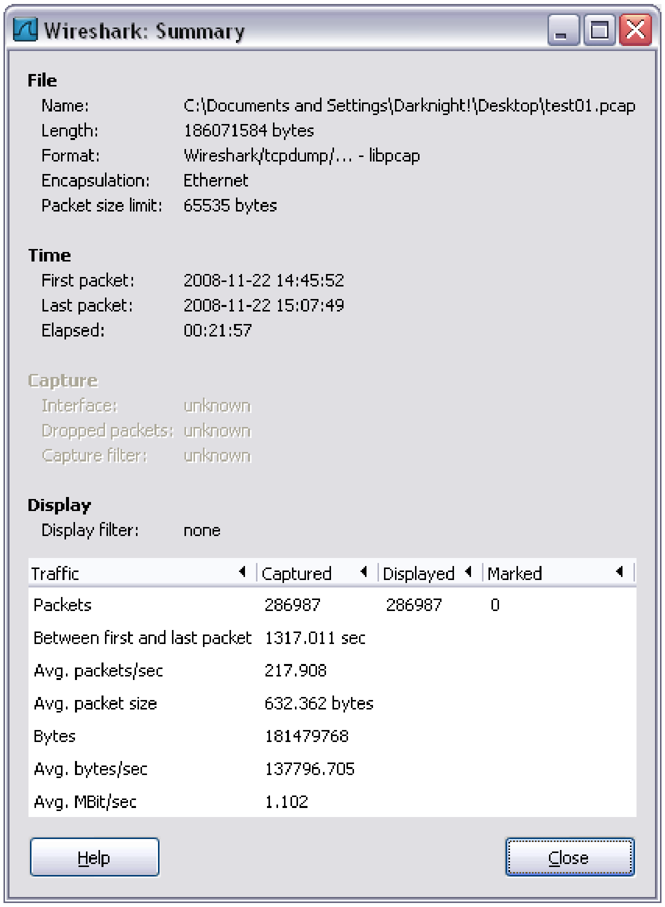


Figure 5.25: MATLAB Plot of Right Steep Turn Maneuver

Wireshark was used to test the performance of the network during the flight test. Two Wireshark capture files were recorded and the results of the two tests are presented below.

The first Wireshark test was for a period of 1,317.011 seconds. During this test period 286,987 packets of data, equivalent to 186,071,584 bytes, were captured at an average of 1.102 MBits/sec. The summary of the test is given in Figure 5.28.



File

Name: C:\Documents and Settings\Darknight!\Desktop\test01.pcap
Length: 186071584 bytes
Format: Wireshark/tcpdump/... - libpcap
Encapsulation: Ethernet
Packet size limit: 65535 bytes

Time

First packet: 2008-11-22 14:45:52
Last packet: 2008-11-22 15:07:49
Elapsed: 00:21:57

Capture

Interface: unknown
Dropped packets: unknown
Capture filter: unknown

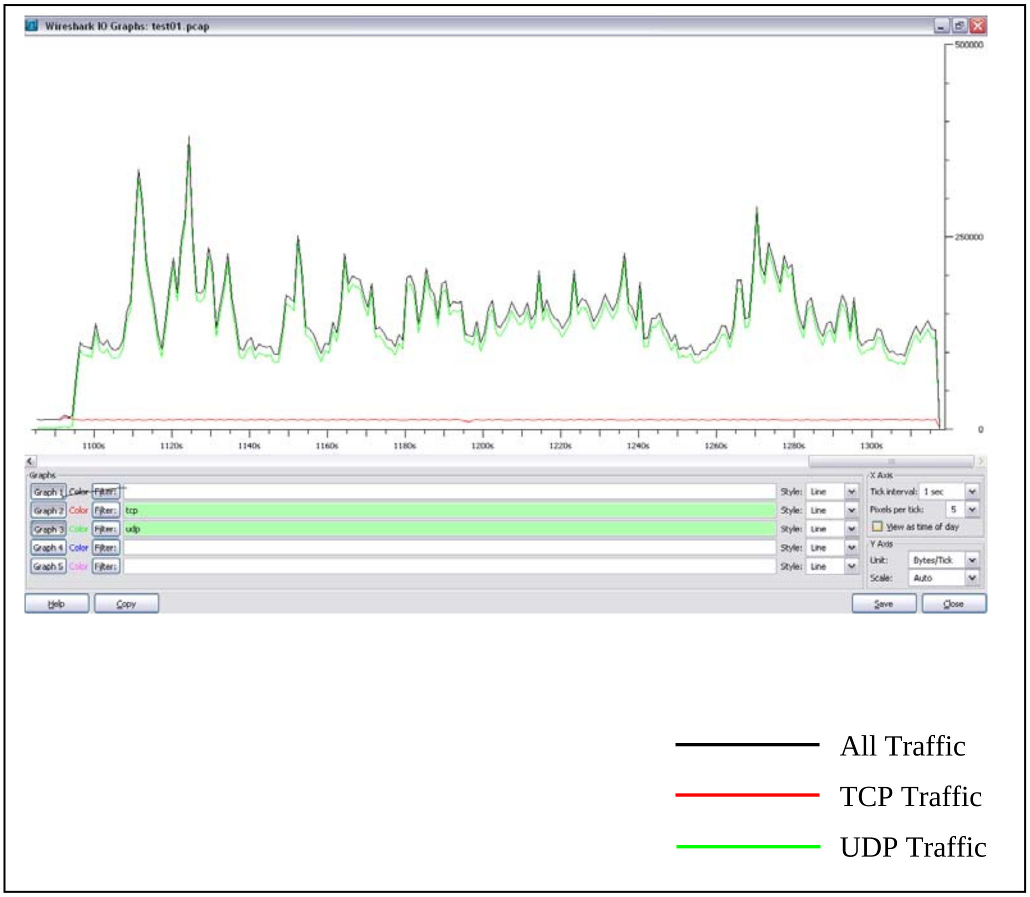
Display

Display filter: none

Traffic	Captured	Displayed	Marked
Packets	286987	286987	0
Between first and last packet	1317.011 sec		
Avg. packets/sec	217.908		
Avg. packet size	632.362 bytes		
Bytes	181479768		
Avg. bytes/sec	137796.705		
Avg. MBit/sec	1.102		

Figure 5.26: Summary of Wireshark Test 01

The I/O graph for the test period shows the transmissions using the Transmission Control Protocol, the User Datagram Protocol and the cumulative of the two. Figure 5.29 shows a section of the I/O graph for the test period. It is seen that the transmissions using the User Datagram Protocol form a major part of the communication. The protocol distribution during the test is summarized in Table 18 and given in Figure 5.30.



Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: tcp Style: Line
Graph 3 Color Filter: udp Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
☐ View as time of day

Y Axis
Unit: Bytes/Tick
Scale: Auto

Figure 5.27: I/O Graph for Wireshark Test 01

Protocol	No. of Packets	Bytes	Percentage
TCP	128,692	167,458,464	44.84
UDP	158,295	14,021,264	55.16
Total	**286,987**		**100**

Table 18: Summary of Protocol Distribution for Wireshark Test 01

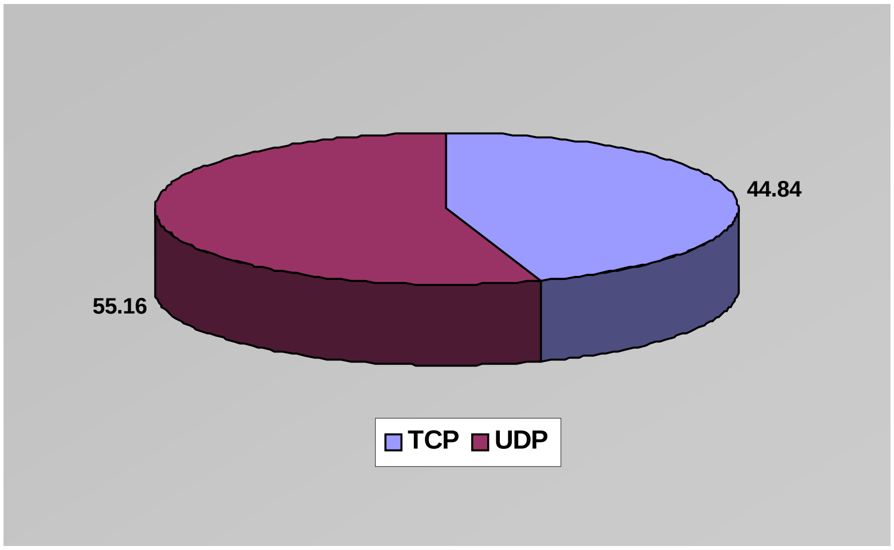


Figure 5.28: Protocol Distribution During Wireshark Test 01

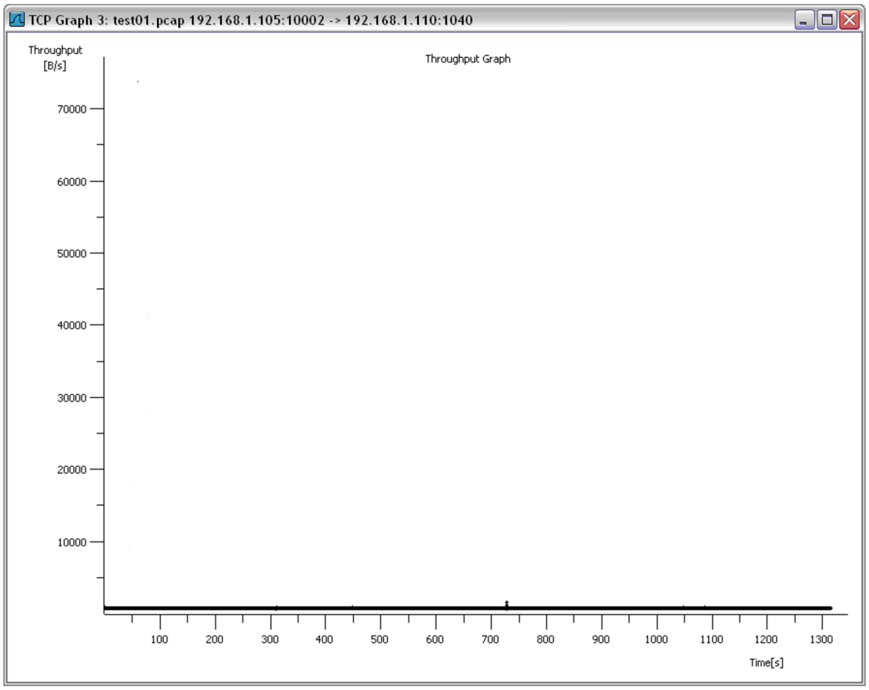


Figure 5.29: Throughput Graph for Wireshark Test 01

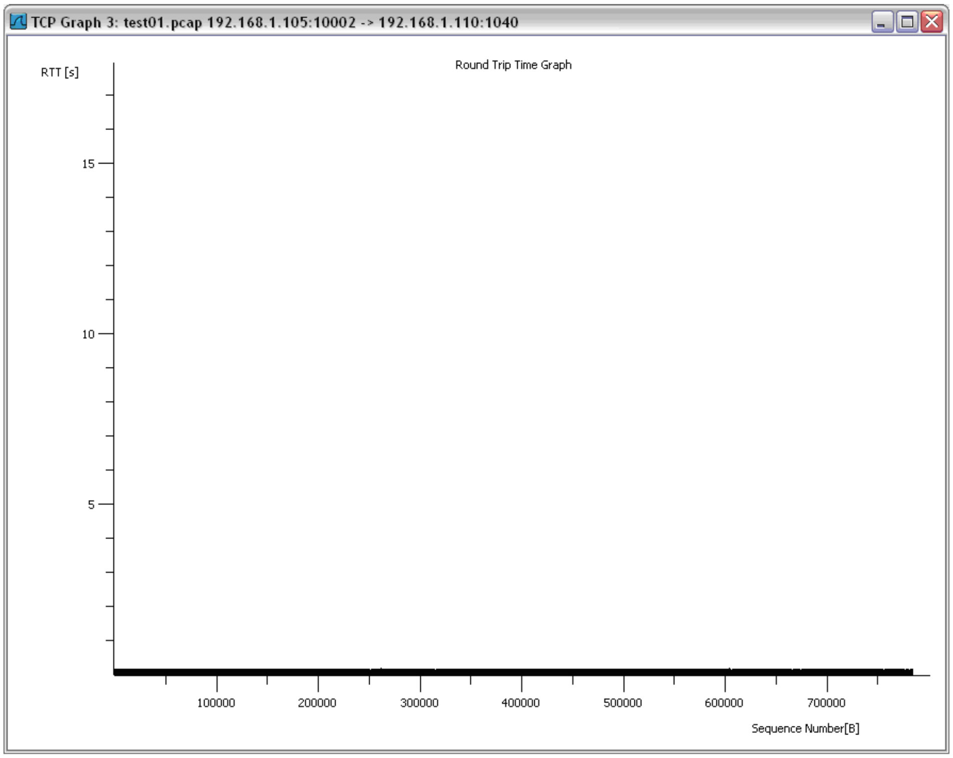


Figure 5.30: Round Trip Time Graph for Wireshark Test 01

Figure 5.31 shows the Throughput Graph and Figure 5.32 shows the Round Trip Time Graph for the test period. The steady and uniform throughput and round trip time indicate that the network performed with no failure. The Time Sequence Graph given in Figure 5.33 shows that the network was congestion free. It was only affected because of the protocol to search and establish connection with all available nodes external to the network.

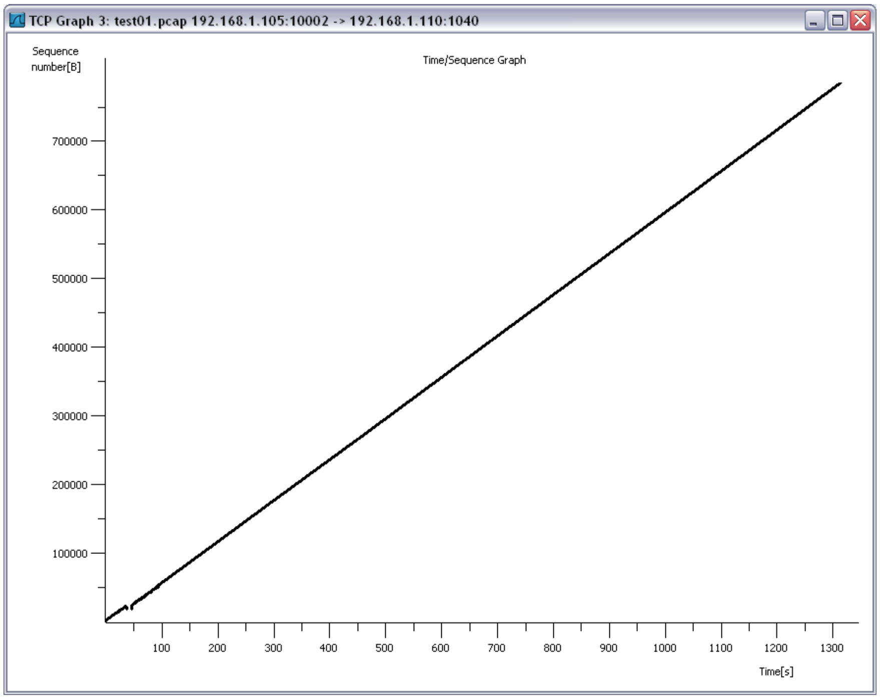
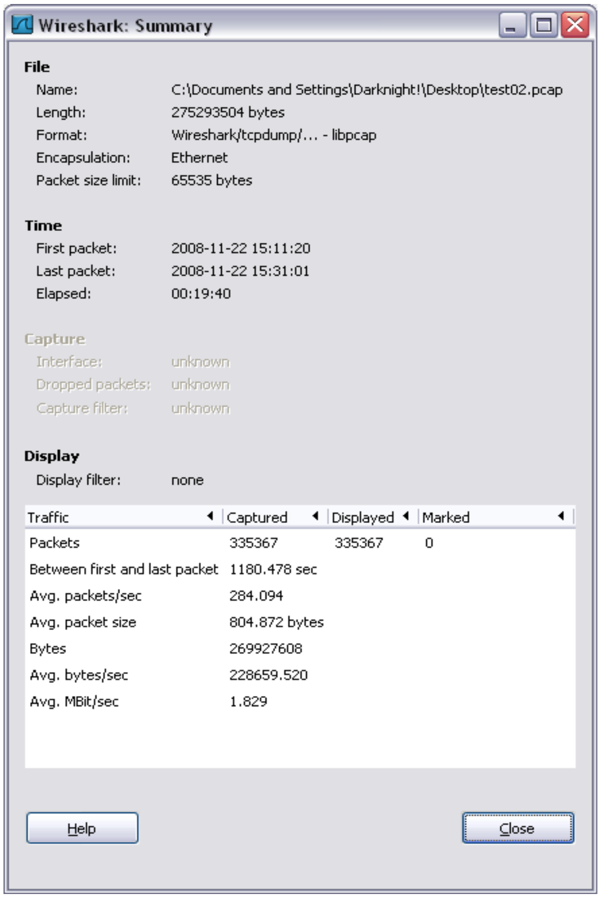


Figure 5.31: Time Sequence Graph for Wireshark Test 01

The second test using Wireshark was conducted for a test period of 1,180.478 sec during which 335,367 data packets, equivalent to 269,927,608 bytes of data, were captured at an average of 1.829 MBits/sec. Figure 5.34 shows the summary of the test.



File

Name: C:\Documents and Settings\Darknight!\Desktop\test02.pcap
Length: 275293504 bytes
Format: Wireshark/tcpdump/... - libpcap
Encapsulation: Ethernet
Packet size limit: 65535 bytes

Time

First packet: 2008-11-22 15:11:20
Last packet: 2008-11-22 15:31:01
Elapsed: 00:19:40

Capture

Interface: unknown
Dropped packets: unknown
Capture filter: unknown

Display

Display filter: none

Traffic	Captured	Displayed	Marked
Packets	335367	335367	0
Between first and last packet	1180.478 sec		
Avg. packets/sec	284.094		
Avg. packet size	804.872 bytes		
Bytes	269927608		
Avg. bytes/sec	228659.520		
Avg. MBit/sec	1.829		

Figure 5.32: Summary of Wireshark Test 02

During this test, the nodes of the network were communicating with each other. The issue pertaining to the performance of the network on account of trying to connect to other nodes can be seen. The Throughput Graph, Round Trip Time Graph and the Time Sequence Graph for the test period are given in Figures 5.35 through Figure 5.37.

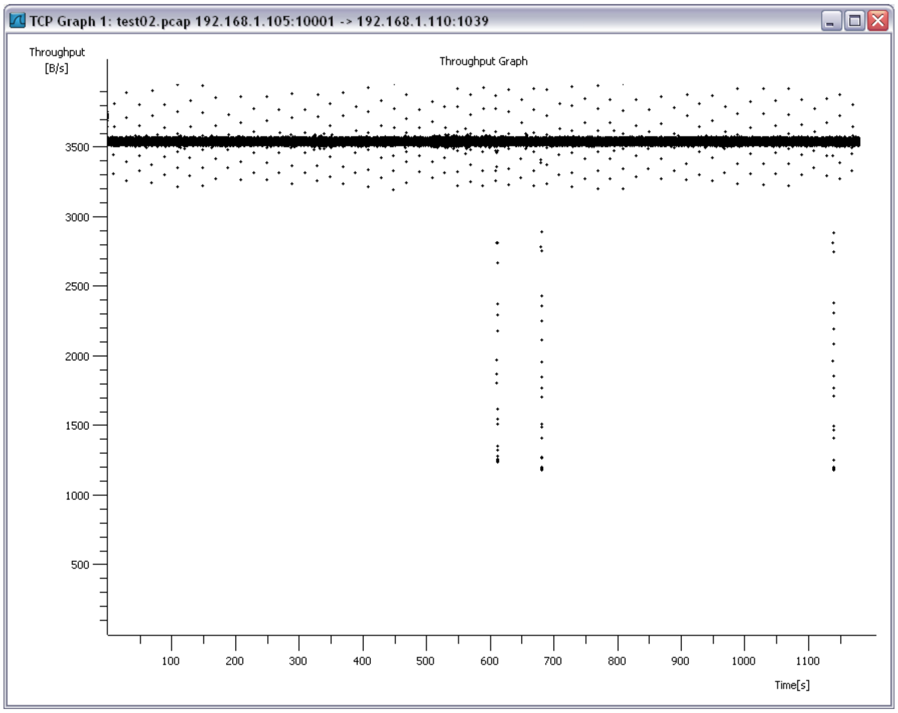


Figure 5.33: Throughput Graph for Wireshark Test 02

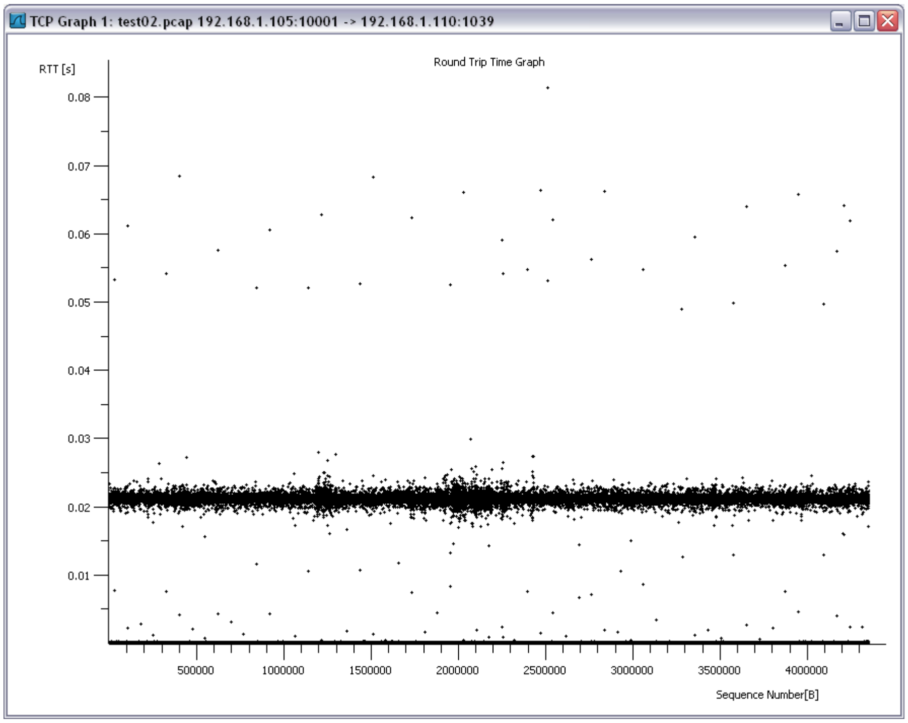


Figure 5.34: Round Trip Time Graph for Wireshark Test 02

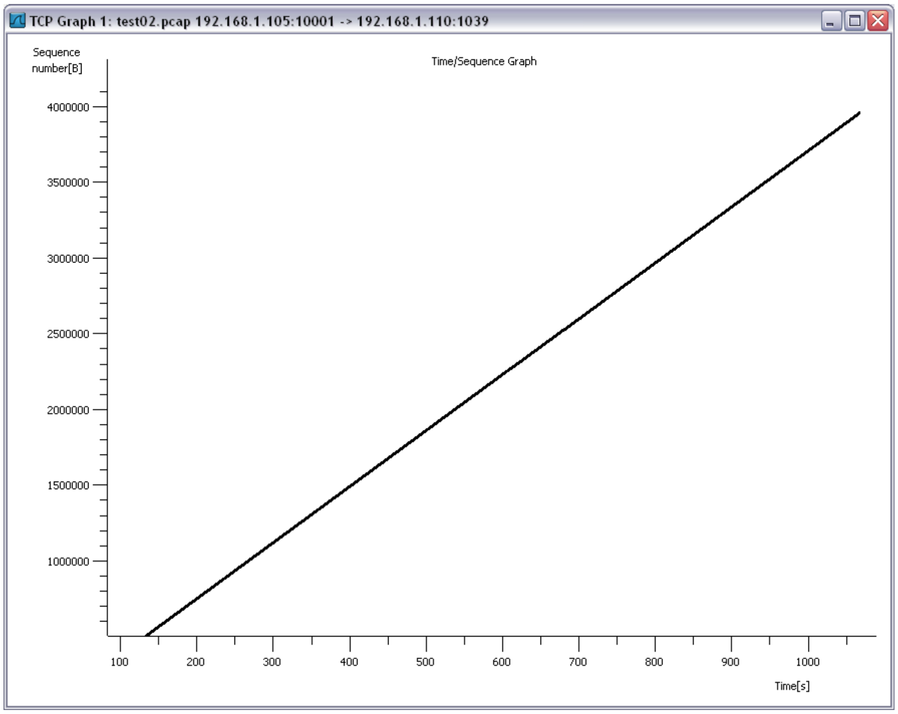
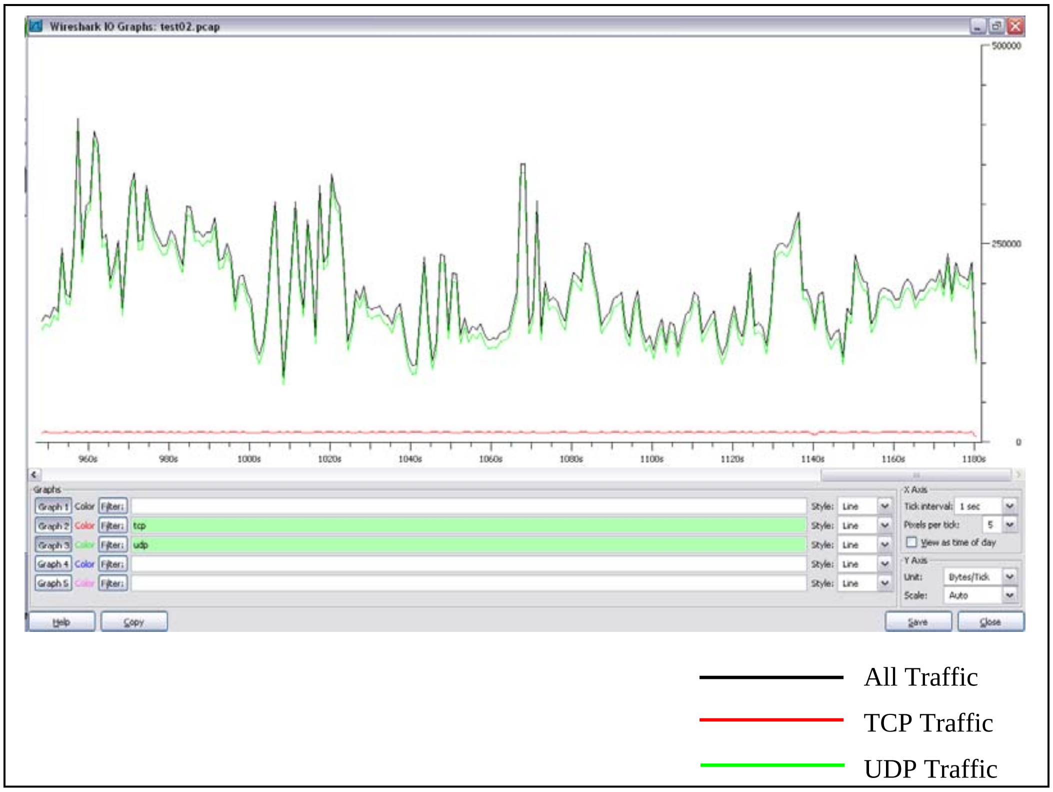


Figure 5.35: Time Sequence Graph for Wireshark Test 02

The I/O graph for this test shows that transmissions from the IP Camera using the User Datagram Protocol make up a large portion of the data and that the data from the W-AHRS using the Transmission Control Protocol is steady and insignificant when compared to the data volume of the IP Camera. It also shows that no communication took place using any other protocol. The I/O graph is given in Figure 5.38, and the protocol distribution for the test is summarized in Table 19 and illustrated in Figure 5.39.



Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: tcp Style: Line
Graph 3 Color Filter: udp Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line

Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day
Unit: Bytes/Tick
Scale: Auto

Figure 5.36: I/O Graph for Wireshark Test 02

Protocol	No. of Packets	Bytes	Percentage
TCP	148,135	13,081,425	44.17
UDP	187,232	256,846,183	55.83
Total	**335,367**		**100**

Table 19: Summary of Protocol Distribution for Wireshark Test 02

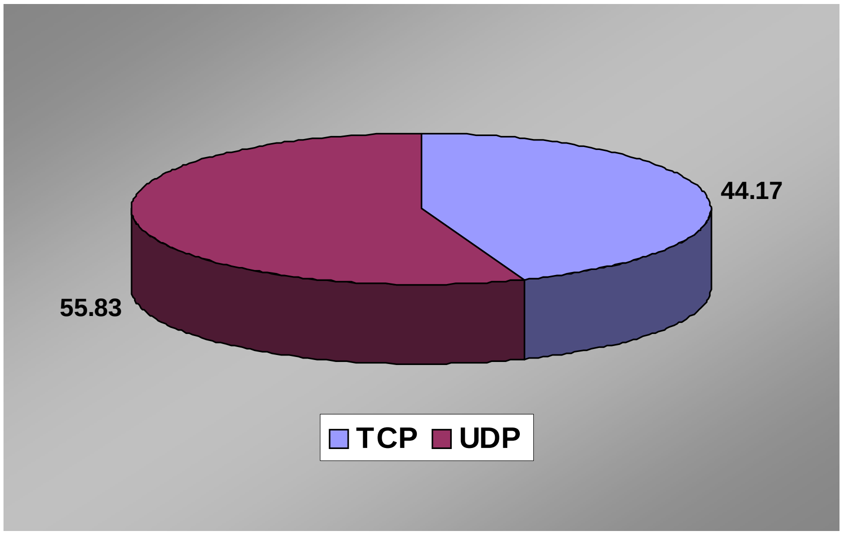


Figure 5.37: Protocol Distribution During Wireshark Test 02

During the flight test, data from the W-AHRS was logged for each maneuver for post flight test processing. The maneuvers performed during the test are usually done to derive the flight dynamics of the aircraft. Data about the attitude of the aircraft was logged and the sensor activity is summarized in Table 20. The log time is the total time it took to complete the maneuver. The NAV 420 was set to transmit NAV packets consisting of pitch, roll and yaw angles, longitude, latitude, altitude, GPS velocity and the angular rates. The number of NAV packets recorded and the average output rate of the sensor is also shown in Table 20.

Flight Maneuver	No. of Packets	Log Time (sec)	Packets/sec (Hz)
Rate 1 Turns	11199	111.981964	100.01
Steep Turns	7488	74.871704	100.01
Short Impulses	6637	66.359381	100.02
Control System Doublets	7386	73.848924	100.01
Sideslips	9317	93.187166	99.98
Slow Flight Turn	5249	52.498168	99.98
Slow Flight	12042	120.408151	100.01
Acceleration	3225	32.233735	100.05
Frequency Sweeps	6481	64.820495	99.98
Total	**69024**	**690.209688**	**100.004392**

Table 20: Sensor Update Rate for Different Maneuvers

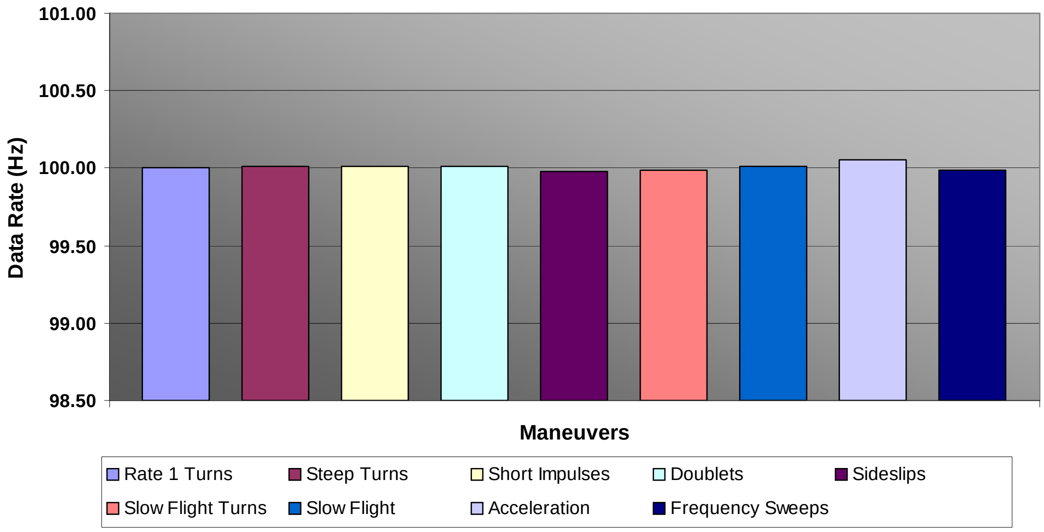


Figure 5.38: Sensor Update Rate

The required sensor update rate depends on the system architecture and the parameter it is measuring and the design of the controller. The NAV 420 showed a consistent update rate of 100 Hz and good performance of the network was demonstrated. It is to be noted that the AHRS units used in many commercial planes have an update rate of 60-100 Hz.

The signal strength of the connection was also tested during flight and the SNR plot is shown in Figure 5.41. Consistent signal strength of approximately -20 dBm reflects good network performance.

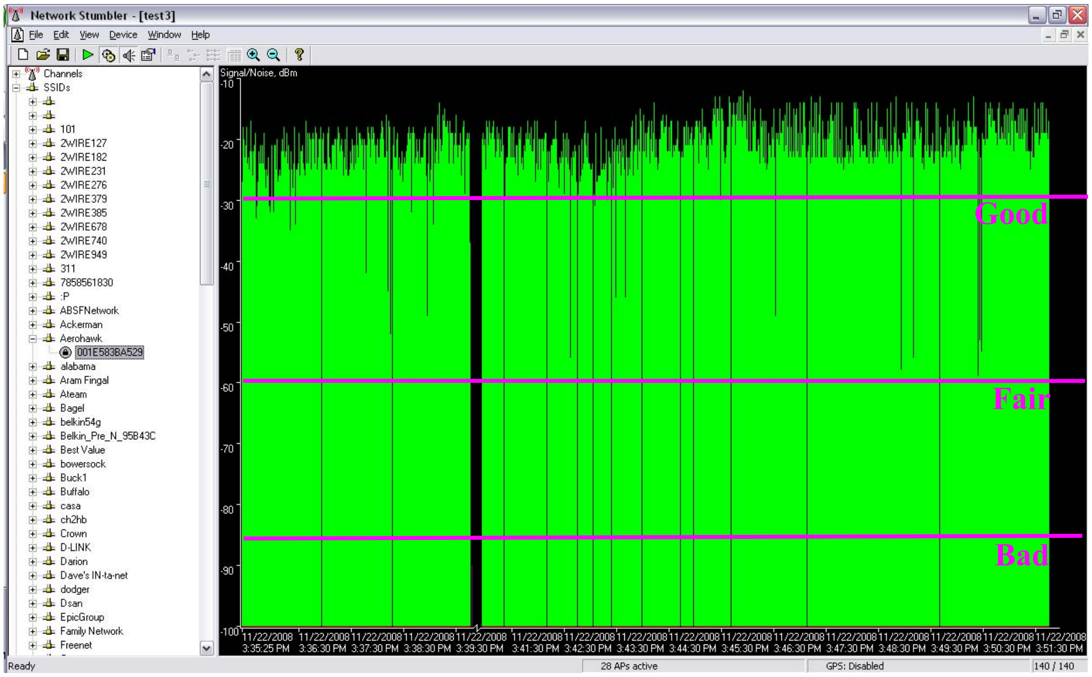


Figure 5.39: SNR Performance Graph during Flight Test

The results from the flight test demonstrate the usability and reliability of a network based on the IEEE 802.11 protocols. The network was very easily installed on the aircraft before the test and was also easily removed from the aircraft after the test. No modification to the aircraft was required to install the equipment and conduct the flight test. The network did not interfere with the functioning of the onboard electronics and the navigation equipment during the test. The signal strength and throughput analysis of the test reflect network availability and indicate a performance that is conducive to application in aviation systems.

6. Ad-Hoc Mode Versus Infrastructure Mode

A comparison of the results from the implementation of the wireless system in the Ad-Hoc mode and the Infrastructure mode is presented in this section.

The Ad-Hoc mode for Wi-Fi connectivity employs devices communicating directly with each other. No Access Point (router) is required for communication between devices. All devices in the range connect in a peer to peer communication mode. This is an easy method for setting up a wireless network and is acceptable for a network that consists of a small number of devices. The throughput of the system is a cumulative of the throughput of the individual nodes. In our testing, the throughput of the entire system was obtained as 0.705 Mbps with wireless adapters that support data rates of up to 54 Mbps. The contribution of the two nodes, the W-AHRS and the IP Camera, was measured to be 0.060 Mbps and 0.645 Mbps respectively. The W-AHRS traffic was in the Transmission Control Protocol (TCP) and the IP Camera employed the User Datagram Protocol (UDP). The protocol distribution for the test, as obtained from IP Tools, is given in Figure 6.1. The figure shows the number of data packets communicated in the UDP and TCP protocols as a percentage of the total number of data packets.

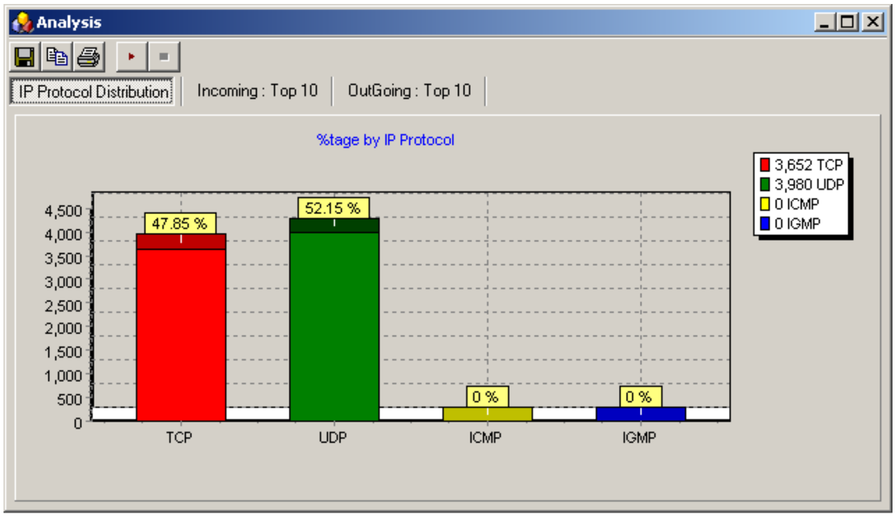


Figure 6.1: Protocol Distribution as a Percentage of Total Number of Packets in Ad-Hoc Mode

The Round Trip Time for the two nodes was also not effected by the presence of the other node in the Ad-Hoc mode. The average Round Trip Time for the system was computed as 0.02 sec and we had a continuous connection to both the nodes, as seen from the Time Sequence Graph given in Figure 6.2.

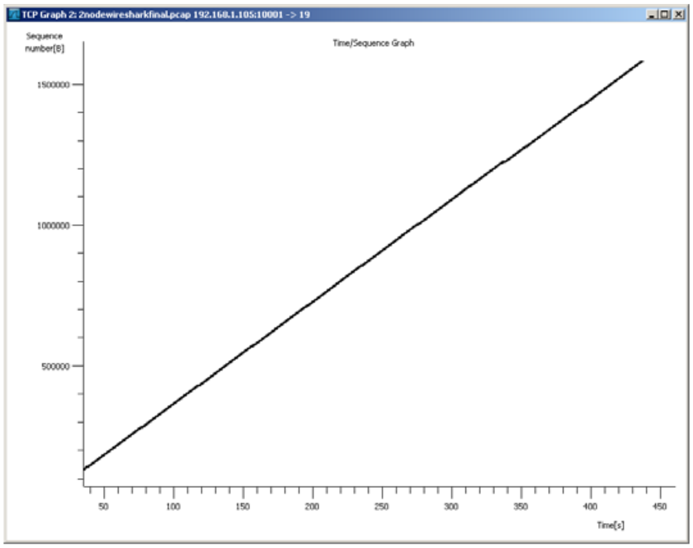


Figure 6.2: Time Sequence Graph for the TCP Traffic in Ad-Hoc Mode

In the Infrastructure mode, the Access Point was included in the network to rout traffic from the W-AHRS and the IP Camera to the User Interface Node. In this set up, the throughput of the system was measured at 1.102 Mbps with 0.085 Mbps from the W-AHRS and 1.017 Mbps from the IP Camera. The protocol distribution during the test is given in Figure 6.3.

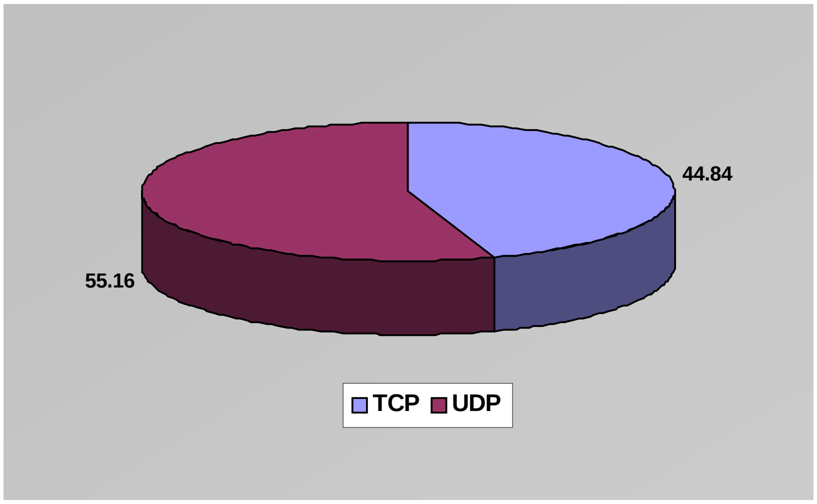


Figure 6.3: Protocol Distribution as a Percentage of Total Number of Packets in Infrastructure Mode

The protocol distribution in the Infrastructure mode is comparable to the distribution observed in the Ad-Hoc mode. Also, the Time Sequence Graph for the test in the Infrastructure mode, given in Figure 6.4, shows the continuity of the communication link.

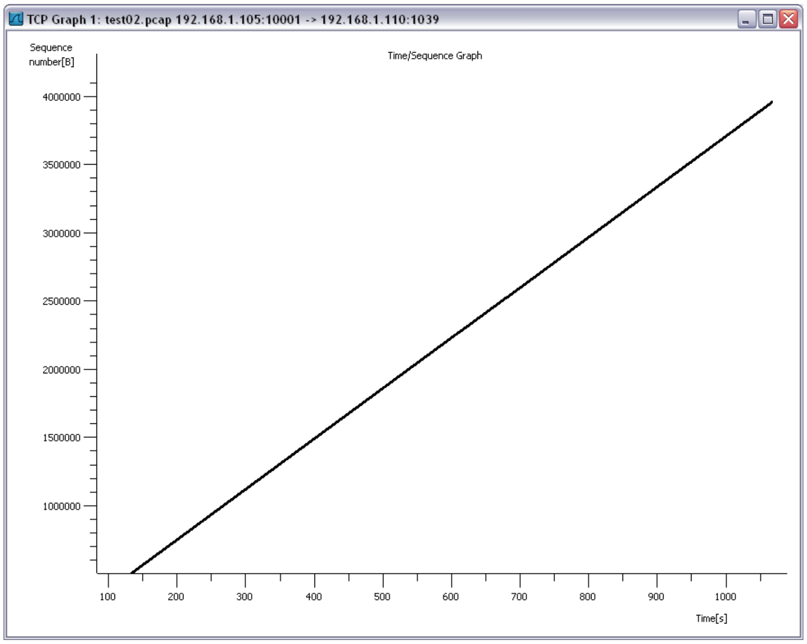


Figure 6.4: Time Sequence Graph for TCP Traffic in Infrastructure Mode

6.1. Discussion

The Ad-Hoc mode and the Infrastructure mode are both viable implementations for the flight test system. From a design point of view, the Ad-Hoc mode presents a convenience similar to the ‘plug n play’ option. However, a disadvantage of using the Ad-Hoc mode is the requirement to keep all the clients within each other’s connecting range. In a large aircraft, connection between multiple nodes can be lost when the sensors reside in areas where there is a considerable distance between them, thus placing the network adapters out of range of each other. Ad-Hoc mode is best used for a small number of devices which are physically present in close proximity with each other and also generate enough traffic to have a high throughput. In the Ad-Hoc mode as the number of devices grows, the performance of the network suffers. Disconnections of devices may occur randomly from time to time and managing the network can be a difficult task. The balance between the number of nodes and the throughput of the system can be achieved through several iterations. During our tests in the Ad-Hoc mode, the operating system in the User Interface Node was configured to not search and respond to any enquires from any access points or nodes other than to the nodes in our network. This feature offered a basic level of filtration to ensure connectivity of the nodes and also led to a better system performance when compared to the flight test results done in the Ad-Hoc mode. During the flight test, there was a loss in connection for 5.8% of the test duration of 776 sec [1]. The inclusion of the IP Camera in the Ad-Hoc mode increased the throughput from 0.059 Mbps to 0.705 Mbps. The disadvantage in considering the Ad-Hoc mode of implementation is that the functionality of the system may be dependent on all the nodes of the system being powered on. A major constraint in employing the Ad-Hoc mode for flight critical systems is that there is no means to control how network resources are shared to fulfill the requirements of such services. A network in the Ad-Hoc mode cannot be programmed to prioritize data transfer for different services within the available bandwidth.

The restrictions arising out of employing the Ad-Hoc mode are overcome in the Infrastructure mode by the inclusion of an Access Point in the network. The Access Point acts as a gateway for all the traffic in the network. By employing the infrastructure mode, the range of operation of a network can be extended by strategically placing the Access Point for maximum reception and range. This is an economical way of extending the range of the network without the use of high gain antennas. In the Infrastructure mode, all the traffic is channeled through the Access Point, hence a larger number of nodes can be included in the network. The Access Point that was employed in our work supports up to 32 nodes in a network.

The major advantage of including an Access Point and considering the Infrastructure mode is the ability to install a Quality of Service (QoS) mechanism. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. The term, Quality of Service, refers to a number of technologies such as Differentiated Service Code Point (DSCP), which can identify the type of data in a data packet and so divide the packets into traffic classes that can be prioritized for forwarding. The benefits of a QoS-aware network include the ability to prioritize traffic to allow critical flows to be served before flows with lesser priority, and greater reliability in a network by controlling the amount of bandwidth an application may use and thus controlling bandwidth competition between applications (the 'babbling idiot' problem). In considering wireless networking for flight critical systems, a major consideration would be the bit rate, delay, jitter, packet dropping probability and/or bit error rate. These parameters can be measured and a desired level of service can be guaranteed by implementing QoS mechanisms in the network. A programmable Access Point provides the ability to make the network a QoS-aware network.

The Infrastructure mode presents the designer with the task to balance between bandwidth utilization, assured quality of service and the size of the network. In our research, we employed two sensor nodes and one User Interface Node. The throughput recorded was 1.102 Mbps against the supported capacity of 54 Mbps. So the network can be extended to include several other nodes. If these nodes include flight critical systems, then an acceptable factor of safety would also have to be included while considering the number of nodes and the capacity of the protocol. An example of such a system could be one in which there are 5 flight critical systems with a combined data rate of 15 Mbps. Including a factor of safety of 1, if 30 Mbps is reserved for flight critical systems, then a further 24 Mbps is available. This available bandwidth may be utilized by including multiple IP Cameras and data recording computers. The processing power required to support the large number of nodes and the associated software are also important considerations in designing such a system.

A sample configuration for a flight test system is presented in Table 21. In the table, a flight test system consisting of 6 IP Cameras, 3 IMUs and 15 vibration sensors is considered for calculating the bandwidth utilization. The contributions of the individual nodes to the network traffic are assumed as shown in the Table.

S. No.	Node	Throughput, Mbps	Quantity	Total Throughput, Mbps
		(A)	(B)	(A*B)
1	IP-Camera[*1]	1.01	6	6.06
2	IMU[*2]	0.06	3	0.18
3	Vibration Sensor[*3]	0.75	15	11.25
			Total =	17.49 Mbps
			Factor of Safety =	2.09

*1: The throughput of an IP Camera transmitting 640x480 pixels at 30 frames per second is assumed = 1.01 Mbps.

*2: The throughput of the IMU, with an update rate of 100 Hz, is assumed = 0.06 Mbps.

*3: The throughput of a vibration sensor sampling at 20 kHz is assumed = 0.75 Mbps.

Table 21: A Sample Configuration of a Flight Test System

7. Summary and Conclusions

7.1. Summary

In our research, the focus was to investigate the development of a wireless flight test system based on the IEEE 802.11 protocols. The developed system that was flight tested consisted of two sensor nodes and it was configured in the Infrastructure mode by the inclusion of an Access Point. A wireless enabled Attitude Heading Reference System (W-AHRS) and an IP Camera are the two sensor nodes. A laptop computer was used as the User Interface Node. MointainScope™ and NAV-VIEW software was installed on it to display flight information including topographic maps, attitude and heading to the pilot and the flight engineer.

The system was developed by first investigating the Ad-Hoc mode architecture. This mode was ground tested and proved to be a quick and effective means to employ wireless sensors. The Ad-Hoc mode showed better performance after configuration changes in the operating system of the User Interface Node which isolate it from other access points. An Access Point was included in the system to investigate the Infrastructure mode. The wireless link performed reliably during the flight test. During the flight test, the pilot observed no interference from the wireless system to the onboard avionics. In the Infrastructure mode improved reliability and network performance were observed when compared with the operation in the Ad-Hoc mode [1].

7.2. Conclusions

The advantages of employing the IEEE 802.11 protocols in avionics and flight test systems include enhanced data rates, flexibility of wireless networks in installation and the weight saved by obviating the wires. Our tests showed a throughput in excess of 1 Mbps. By comparison, the popular ARINC 429 data bus has a maximum bit rate of 100 Kbps while the ARINC 629 supports a slightly higher bit rate of 2Mbps. The inclusion of an Access Point and testing the network in the Infrastructure mode is a viable method to designing and developing wireless flight test systems. The inclusion and testing of the IP Camera proved the viability of developing a system that provides video recording as a service in an aircraft. The use of Commercially-available-Off-The-Shelf (COTS) hardware and software greatly reduced the development cost of the wireless flight test system. It is very easy to install wireless communication based instrumentation on the aircraft for flight testing. Unlike proprietary aviation data communication standards, standards like the IEEE 802.11 are inexpensive to implement. Wi-Fi will save on the costs involved in the miles of copper wiring, in the airframe modifications, and in the man-hours required for installations.

8. Future Work

The tests conducted in this work employed rudimentary tools to prove the viability of IEEE 802.11 a/b/g protocols for flight test application. The functionality of the wireless network has to be proved with further testing to establish the performance of a multiple wireless sensor network. The IEEE 802.11 protocols support data rates of up to 54Mbps. We recorded a throughput of 1.102 Mbps with an IP Camera and a wireless enabled NAV 420. So a network with more number of nodes and with a combined data rate that is within the range of the protocol should be developed and tested. As an example, a system with 6 IP Cameras (1 each at the end of each wing, 1 each at the end of the horizontal stabilizer, 1 on the rudder, 1 in the nose cone), 2 NAV 420 IMUs and an array of vibration sensors that are spread across the wing and the fuselage can be considered for evaluating the performance of the network.

The Access Point used in our research supports up to 30 clients. The performance of a network should also be evaluated when the number of nodes in the network is equal to the number supported by the Access Point. The performance of the network should be evaluated to understand the relation between the number of clients and the data rate of the clients. For example, one possible network could be a configuration with 30 nodes each contributing 0.060 Mbps like our W-AHRS did. Another possible network could be a configuration of limited nodes, say 5, with each contributing about 10 Mbps to the total network traffic.

If the designer is inclined to using the Ad-Hoc mode, then iteration on the number of nodes to be used and their individual data rates will be required to design the optimum system. Also, if such a system is operated along with a network in the Infrastructure mode, the performance of the Wi-Fi systems has to be evaluated. For example, the network in the Infrastructure mode could include all the instruments for the pilot while the network in the Ad-Hoc mode could include a data acquisition computer and an array of strain gauges.

During flight testing of the network, all the nodes of the network were present in the cabin. Though there was no line of sight, there were no metal obstacles between them either. In an actual flight application the performance could change considerably with the location of the wireless instruments. Also, the use of high gain antennas in such an environment should be investigated. High gain antennas and sensitive receivers improve the signal strength and lead to better data transmission rates.

A thorough analysis of the network would require trace capture at the sender and the receiver end. The network should be examined with tools and procedures that are able to quantify the free space path losses and the path losses within the aircraft. This would help evaluate the performance of the network against the system requirements.

The Infrastructure mode should be tested with a Quality of Service (QoS) programmable Access Point. This would enable the investigation of employing wireless protocols for flight critical systems as mechanisms can be employed to ensure network specifications meet the requirements of such critical systems.

The RF environment within the aircraft should be studied for a better understanding of the interference to and from an avionics network. Extensive flight testing of the Wi-Fi system is required on aircraft that have complex electronic flight instrument systems.

9. References

1) Satish Chilakala, “Development and Flight Testing of a Wireless Avionics Network Based on the IEEE 802.11 Protocols”.
2) Michael Gandy, Lockheed Martin: Wireless Sensors for Aging Aircraft Health Monitoring.
   URL: http://www.jcaa.us/AA_Conference_2001/Papers/7B_2.pdf.Lockheed Martin Structural Health Monitoring
3) http://www.honeywell.com
4) http://www.securaplane.com/index.html
5) http://www.flightdeck.aero/flightdeck-q10053-c10043-SkyFi_2000.aspx
6) http://www.avtoday.com
7) http://www.teledyne-controls.com
8) http://www.avionica.com
9) http://www.geaviationsystems.com/News/Archive/2009/Reducing-W/index.asp
10) http://www.xbow.com/Products/iproductsoverview.aspx
11) http://www.lantronix.com/device-networking/external-device-servers/wibox.html
12) http://www.axis.com/products/cam_211w/index.htm
13) http://www.ampro.com/Products/ReadyBoard/
14) http://www.mesanet.com/
15) http://www.adlinktech.com/ampro-extreme-rugged/index_ampro.html
16) http://www.dlink.com/WBR-1310
17) Dryden Flight Research Center: “Radio-Frequency Wireless Flight-Control System”.
    URL:http://www.dfrc.nasa.gov/Newsroom/Xpress/1999/Mar26/news.html.
18) http://www.invocon.com/WFCS_tech_overview.html.
19) http://www.ueet.nasa.gov/toi/viewtoi.php?id=98.
20) http://www.honeywell.com/sites/aero/Communication_Navigation_Systems3_C2 BB6B07D-BE5D-1863-8A9A-D7F4A616C4EC_H3286B641-92EB-BB9B-8960-148D029122C0.htm.

21) White Paper – Securaplane Technologies Inc.: SecuraNet™ WIRELESS TECHNOLOGY Intra-Aircraft Wireless Data Bus for Essential and Critical Applications.

22) Tom Karygiannis, Les Owens, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, Special Publication 800-48, National Institute of Standards and Technology.

23) “IEEE 802.11b Wireless LANs”, 3Com Corporation.
URL: http://www.3com.com/other/pdfs/infra/corpinfo/en_US/50307201.pdf

24) “Introduction to IEEE 802.11”.
URL: http://www.intelligraphics.com/articles/80211_article.html

25) Mark Prowten, “Encryption Technology for Embedded Network Devices”, Industrial Ethernet Book Issue 26:31.
URL:http://wireless.industrial-networking.com/articles/articledisplay.asp?id=514109

26) “Encryption and Its Importance to Device Networking”, Lantronix Inc.

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

28) Windows Platform Design Notes: “Wi-Fi Protected Access (WPA) Overview”.

29) Wi-Fi Alliance: “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks”, April 29, 2003.

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

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

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

33) “Wi-Fi Protected Access 2 (WPA2) Overview”, The Cable Guy, May 2005.

34) “Advanced Encryption Standard Fact Sheet”, January 28, 2002.

35) URL: http://csrc.nist.gov/CryptoToolkit/aes/

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

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

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

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

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

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

42) 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.

43) 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.

44) 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.

45) 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.

46) 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.

47) Mustafa Ergen: IEEE 802.11 Tutorial, June 2002.

48) 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.

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

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

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

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

Appendix A: Flight Test Safety Report

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

Flight Test 01- Safety Report
(Revision: A)

Flight Experiment	Performance Testing of Wireless Avionics System
Date	: 22 November, 2008
Submitted by	: Pradeep Attalury
Team:	
Flight Test Engineer	: Pradeep Attalury
Vehicle/Instrumentation Engineer	: Pradeep Attalury
Vehicle/Instrumentation Engineer	: Dileep Bhogadi
Test Pilot	: Ron Renz

Dr. David R Downing
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.

Pradeep Attalury

Safety Board Certification

Signature: ________________________________
Richard Colgren

Signature: ________________________________
David Downing

Signature: ________________________________
Ron Renz

Revisions

	Date Submitted
Original Version	11/21/2008
Revision A	11/22/2008
Revision B	_________
Revision C	_________
Revision D	_________

Test Overview

The purpose of the flight test described in this document is to demonstrate and test the performance of a three node wireless avionics network. The three node network is connected wirelessly by an IEEE 802.11g link that is established using a wireless router. Of the three nodes, one is a sensor node that incorporates a GPS and an Attitude, Heading Reference System (AHRS). The second node is a Wi-Fi enabled IP Camera and the third 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 of 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 three 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 22nd November 2008. Flight test is proposed to be carried out any time between noon and dusk, 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--VNE: 182 MPH (May not be exceeded at any time.)
- Maximum Structural Cruising Speed--VNO: 145 MPH (Only exceed in smooth air.)
- Minimum Speed (Power off Stall), Clean Configuration--VS1: 57 MPH
- Minimum Speed During Flight Test--1.3VS1: 74.1 MPH (Giving a safety factor of 1.3)

Appendix A.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.

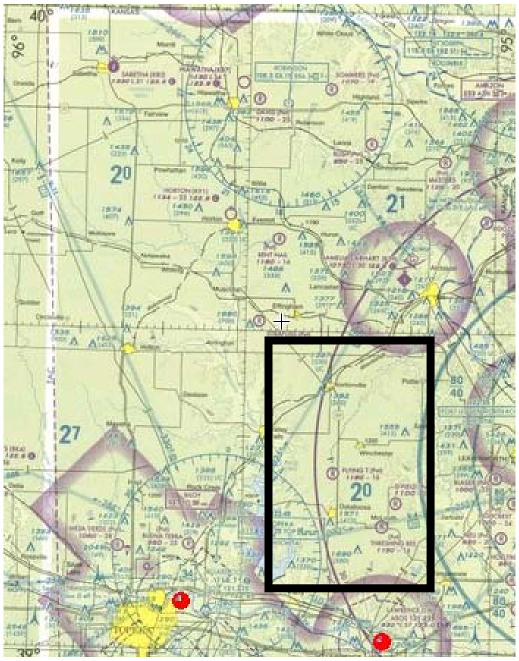


Figure 1: Test Area

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.
- An AXIS® Wi-Fi enabled IP camera (Video Node)
- A wireless router
- A 12 Volt 7.0 Amp Hr Battery, power source for the IP Camera and the wireless router.
- 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. The wireless router will be stowed, all through the flight, in the space available at the back of the pilot's seat. During flight, the IP Camera will be held by the engineer seated beside the pilot. It will be stowed in the back of the co-pilot's seat during take off and landing. The 12V 7Amp Hr battery that powers the router and the IP Camera will be securely attached to the foot of the rear seat of the aircraft. The engineer in the rear seat will have access to it, to disconnect the terminals should the need arise. 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.
- Hold the IP Camera.

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 no more than 1.5 aircraft operating hours to complete, therefore the rental cost will not exceed $150. Equipment required for the wireless avionics network has already been purchased and will require no additional funding. The source of funding for the flight test is the ADMRC 2008 project 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 Cards

1	EMI Check
A	COMM Check
B	NAV Check
2	Take Off
	Normal Take Off, 10deg 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 Turns
	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, Center
B	Elevator Down, Up, Center
C	Rudder Left, Right, Center
D	Rudder Right, Left, Center
E	Aileron Up, Down, Center
F	Aileron Down, Up, Center
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 110 mph IAS
A	Left 20° bank, 90° degree heading change
B	Right 20° bank, 90° degree heading change
10	Slow Flight
A	Flap 10, Altitude 3000ft, Speed 75mph IAS
B	Flap 20, Altitude 3000ft, Speed 75mph IAS
C	Flap 30, Altitude 3000ft, Speed 75mph IAS
D	Flap 40, 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**	
A	**Pre-Flight Procedures**	
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**	**11C**
2	**Barometric Pressure**	**330149**
3	**Winds**	**Clear**
4	**Ceiling/Visibility**	**10 miles**
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:	0 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:	10 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:	30 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:	40 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	□
Land	□
Shut Down	□

Post-Flight Procedure

1. Hobbs Time ____________________
2. Tach Time ____________________

Appendix A.C: Weight and Balance

The table below gives the weight and balance distribution for the test.

	WEIGHT	ARM	MOMENT
EMPTY WEIGHT As Weighed 17 August 2005	1429.8	39.1	55911.13
pilot	170	37.0	6290
FTE #1	170	37.0	6290
FTE #2	130	73.0	9490
FTE #3	0	73.0	0
	1899.8	41.0	77981.13
ADD CARGO			
at REAR SEAT	0	73.0	0
at REAR BAGGAGE	0	95.0	0
at REAR of Pilot's seat (Router+Power Regulator + Camera)	1	40.0	40
at REAR of Co-Pilot's seat (Laptop Computer)	8	46.0	368
at front left corner of Rear seat (Battery, 12V 7Amp Hr)	5	68.0	340
at Baggage bay (Nav420+12V 5Amp Hr Battery + WiBox in black box)	15	85.0	1275
		123.0	0
ZERO FUEL WEIGHT	1928.8	41.5	80004.13
ADD FUEL (FULL = 65 gals)	228	47.8	10893.33
T/O WEIGHT	2156.8	42.1	90897.46
GROSS WEIGHT	2300		

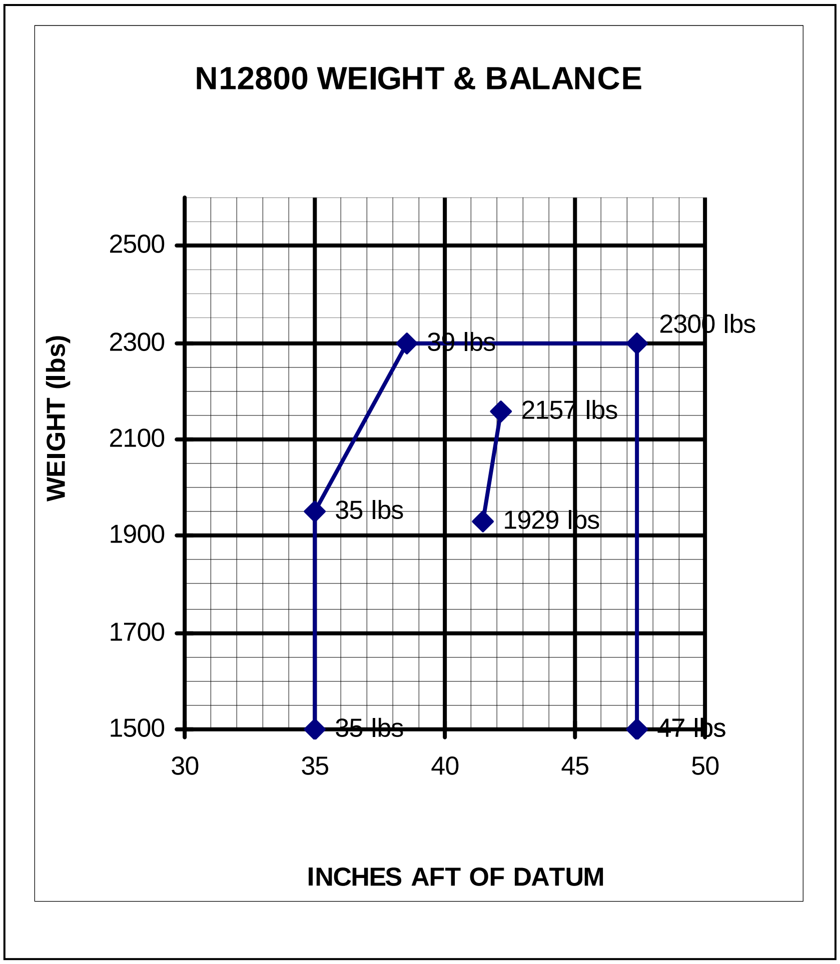


Figure C1. N12800 Weight and Balance

Appendix D: Flight Envelope

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

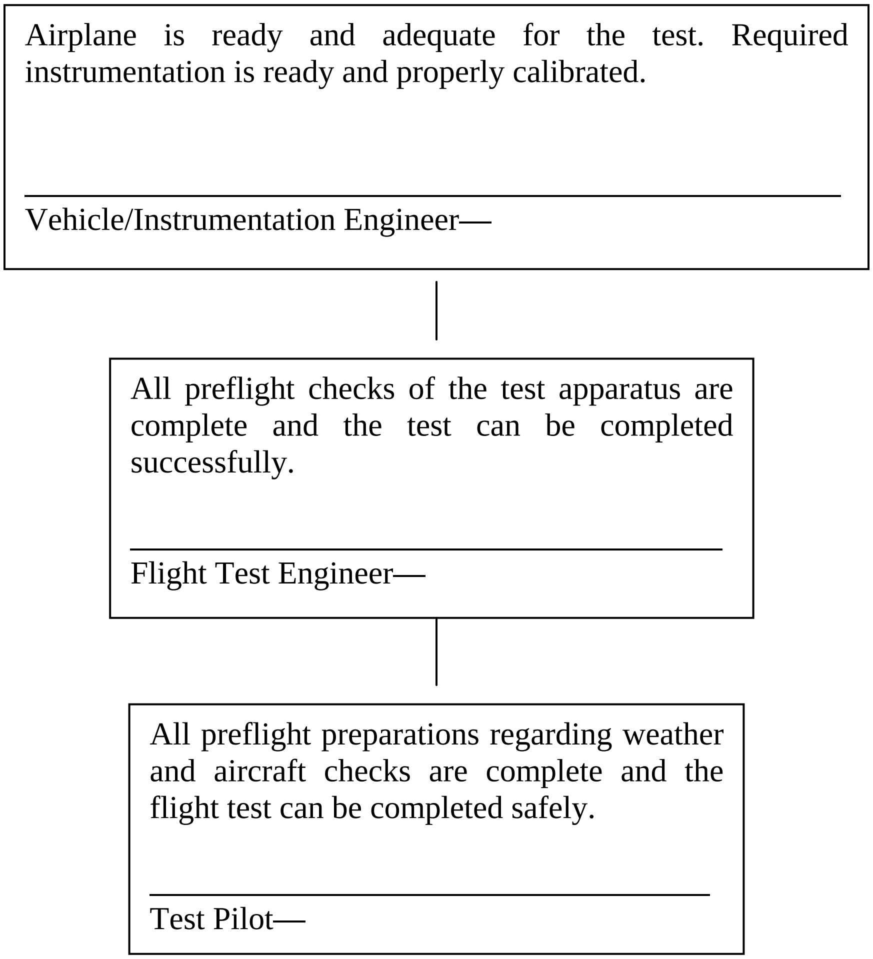
Since the flight envelope and the weight and c.g. limits of the test aircraft will not be exceeded during the specified test flight, and no modifications are being made to the aircraft and its systems, this flight test is classified as low risk.

Conformity Inspection Requirements:

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

Appendix 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.

____

Vehicle/Instrumentation Engineer—

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

____

Flight Test Engineer—

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

____

Test Pilot—

Appendix 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 □

IP camera functional and set to go □

Router functional and set to go □

Fuel Tanks Full □

Vehicle/Instrumentation Engineer

Date

Appendix B: Flight Test Maneuvers

This section gives the results of the various flight maneuvers, continued from Chapter 5. The figures given in this section are obtained by overlaying the raw unfiltered data on Google Earth and the graphical plots are obtained using MATLAB. The data was logged for each maneuver during the flight test.

Figures B-1 and B-2 show the flight track of the Rate 1 turn to the left and to the right respectively. Their corresponding plots drawn using MATLAB are given in Figure B.3 and Figure B.4. A standard rate 1 turn takes about 2 minutes to complete a 360° heading change. The maneuver was conducted at 3,000 ft altitude and 110 mph IAS. It took about 60 seconds to complete a 180° heading change.

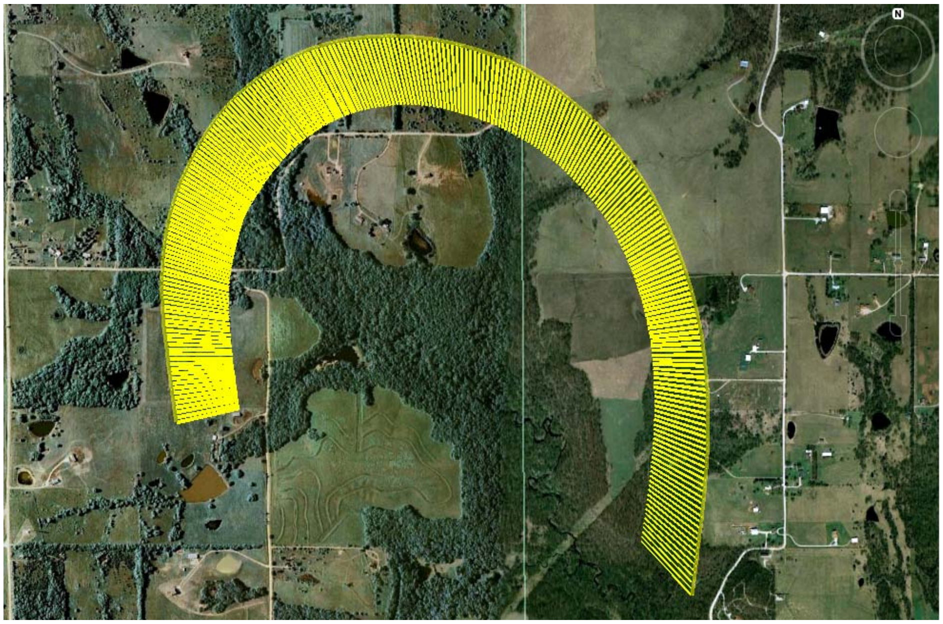


Figure B- 1: Google Earth Screenshot of Rate 1 Turn (Left)

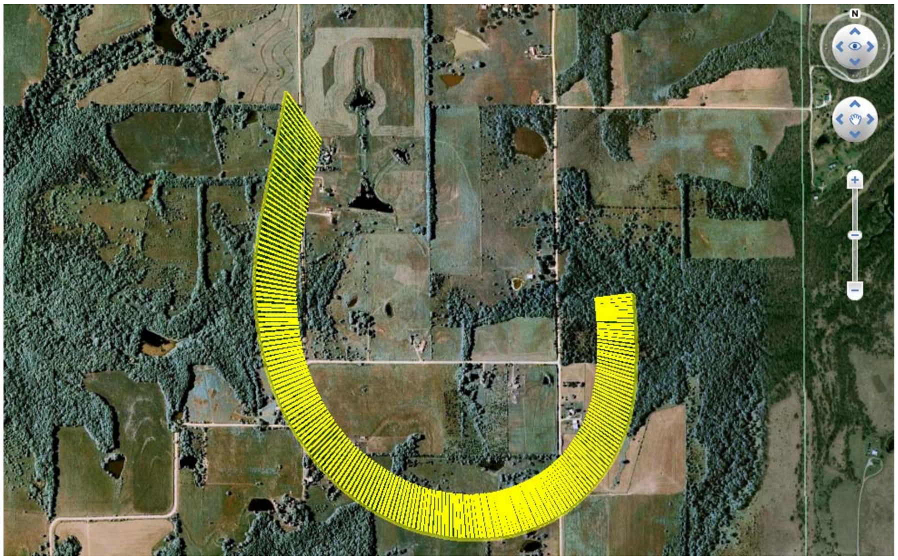


Figure B- 2: Google Earth Screenshot of Rate 1 Turn (Right)

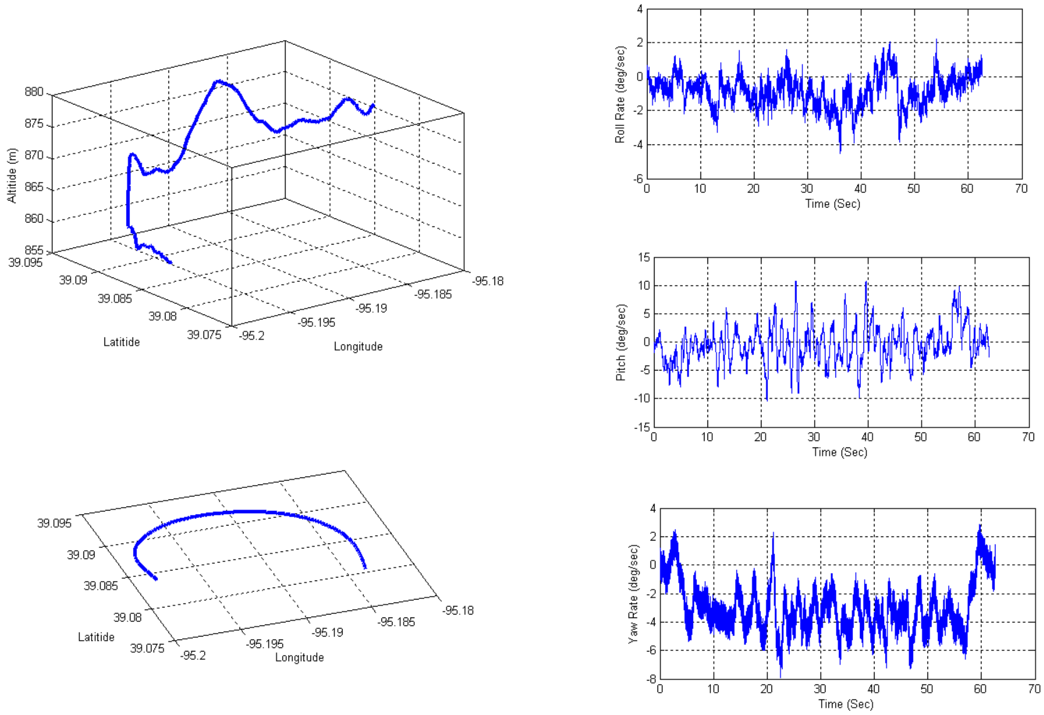


Figure B- 3: Rate 1 Turn (Left)

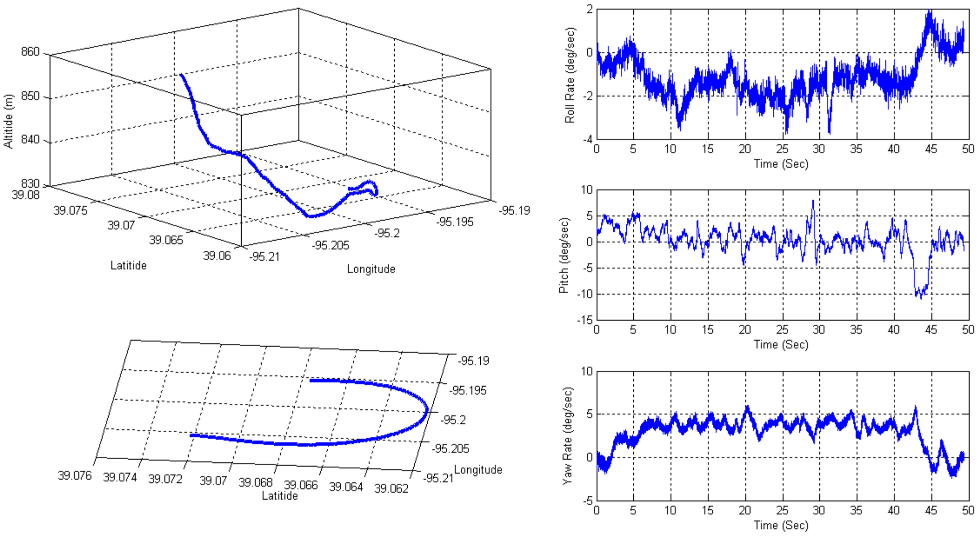


Figure B- 4: Rate 1 Turn (Right)

Figure B-5 shows the flight track of the steep turn to the left and right. Figures B-6 and B-7 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.

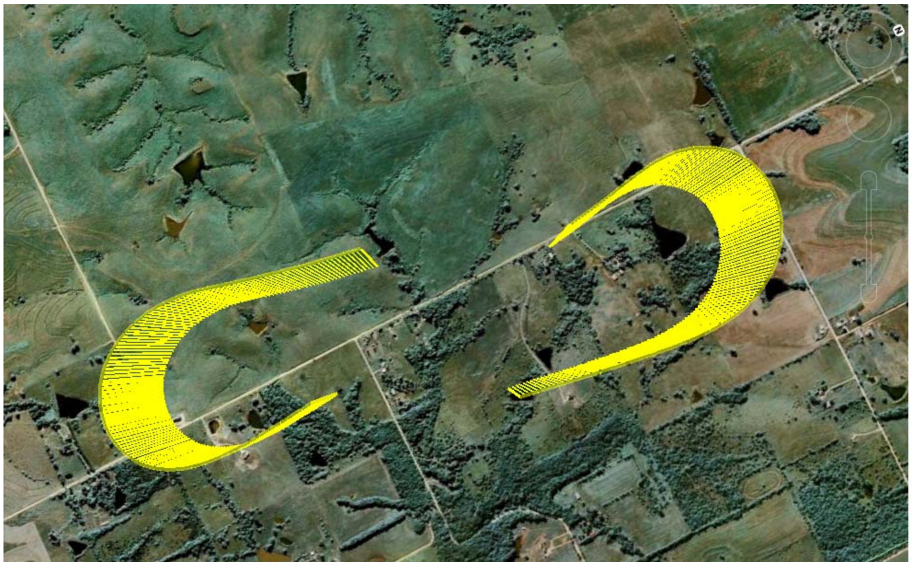


Figure B- 5: Google Earth Screenshot of Steep Turn (Left and Right)

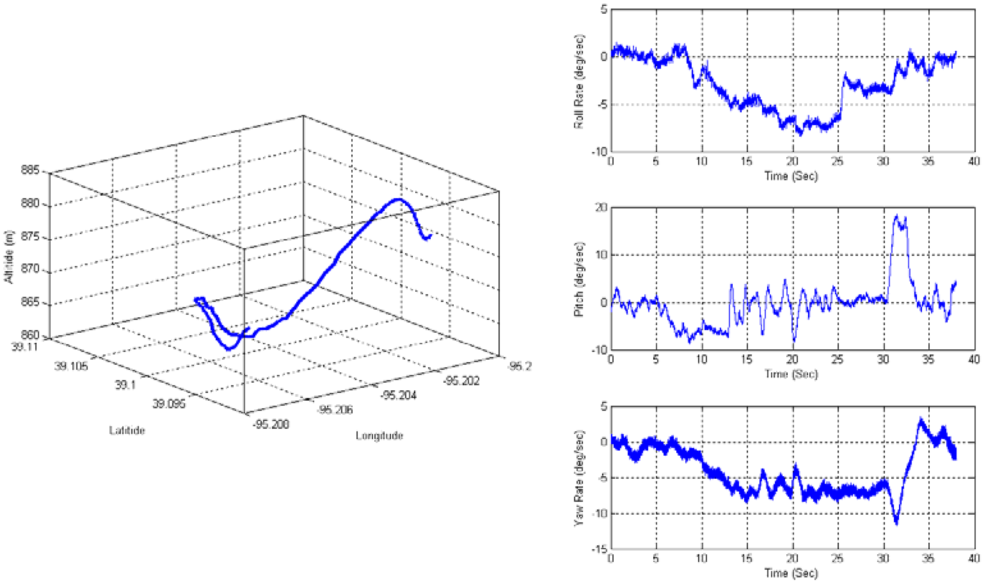


Figure B- 6: Steep Turn (Left)

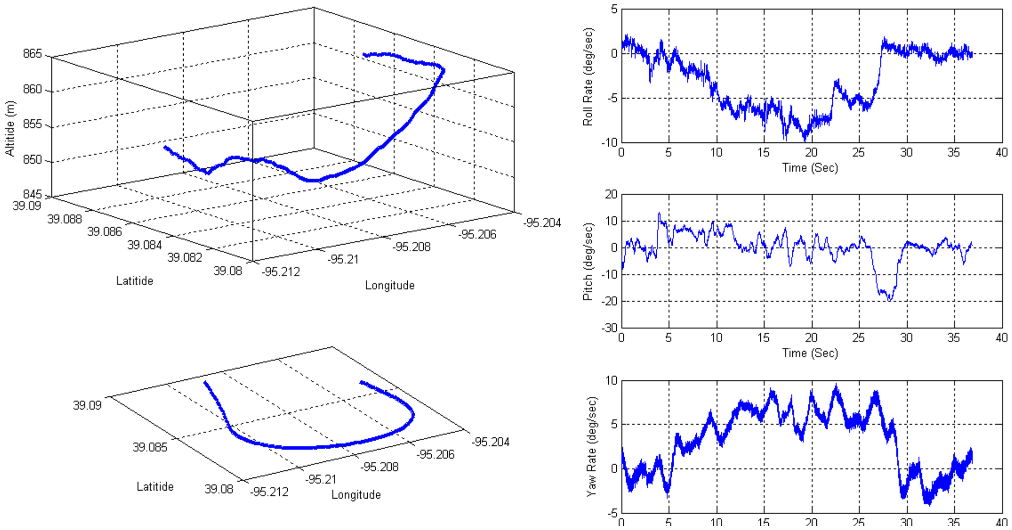


Figure B- 7: Steep Turn (Right)

Figures B-8 through B-11 show the flight track and MATLAB results during short duration impulse command to the elevator. At an IAS of 110 mph and 3000 ft altitude, the pilot commanded approximately 15% of the maximum elevator deflection for 1 second and allowed the airplane to settle before the next maneuver.

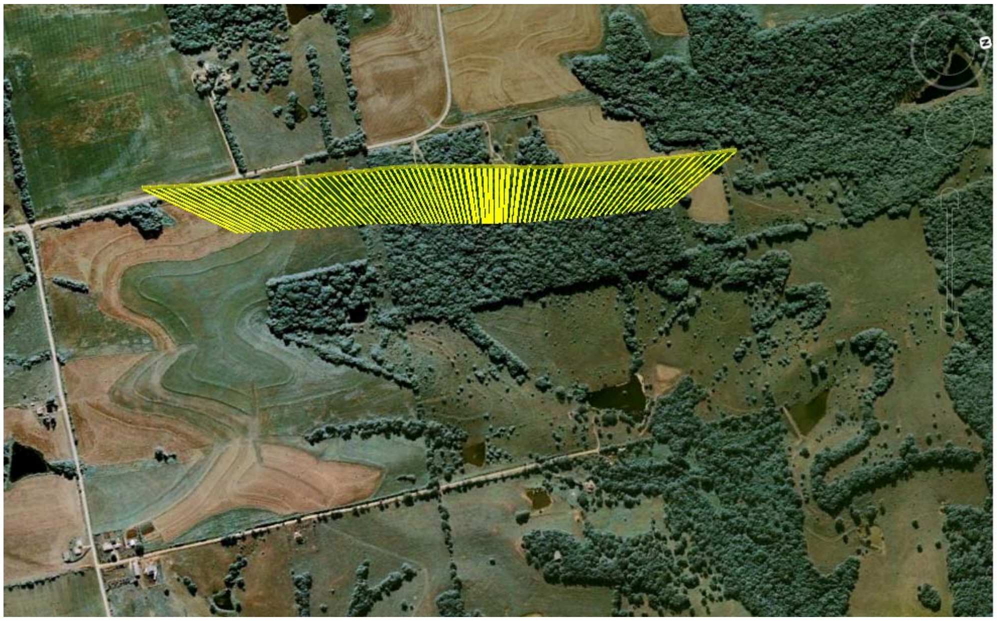


Figure B- 8: Google Earth Screenshot of Short Impulses (Elevator Up)

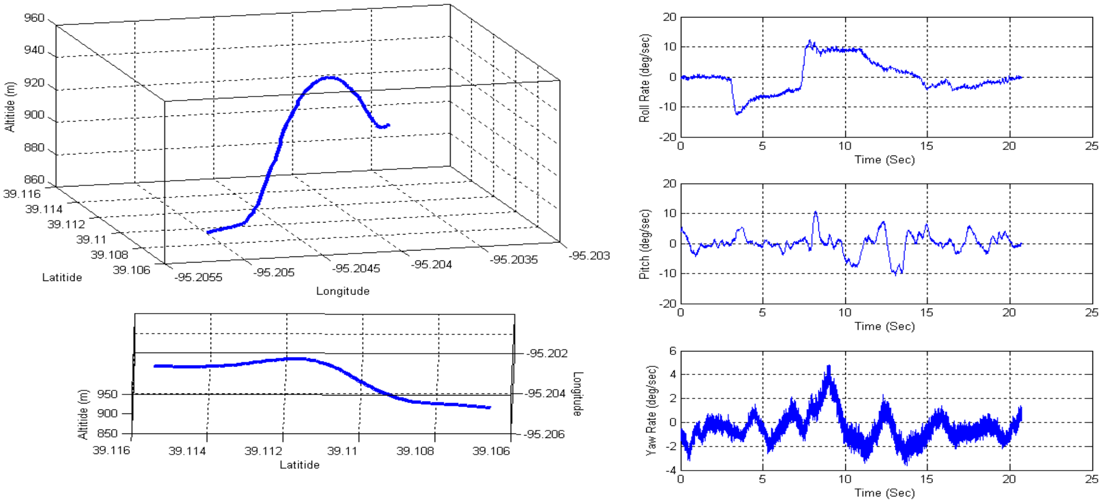


Figure B- 9: Short Impulses (Elevator Up)

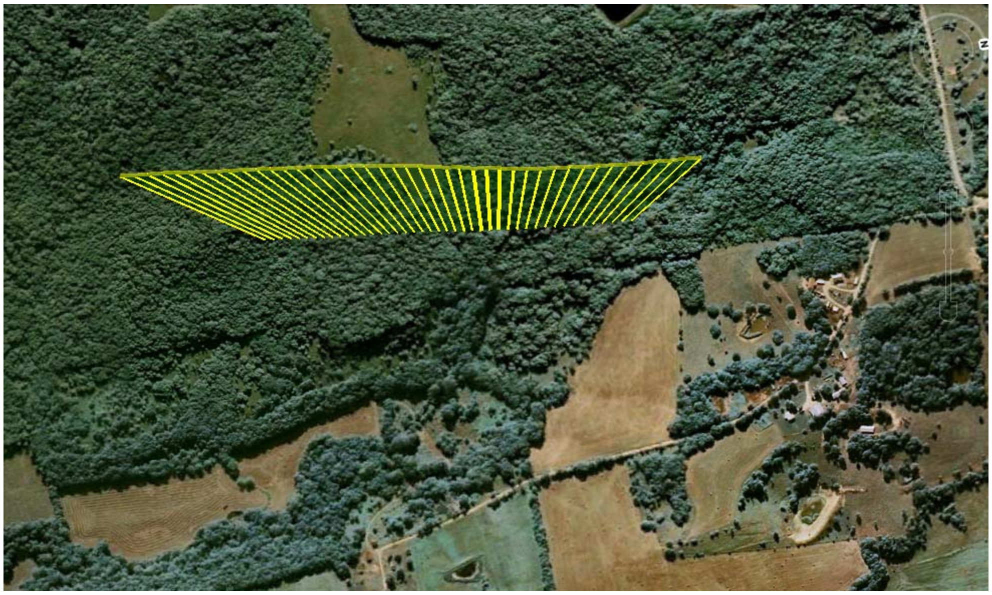


Figure B- 10: Google Earth Screenshot of Short Impulses (Elevator Down)

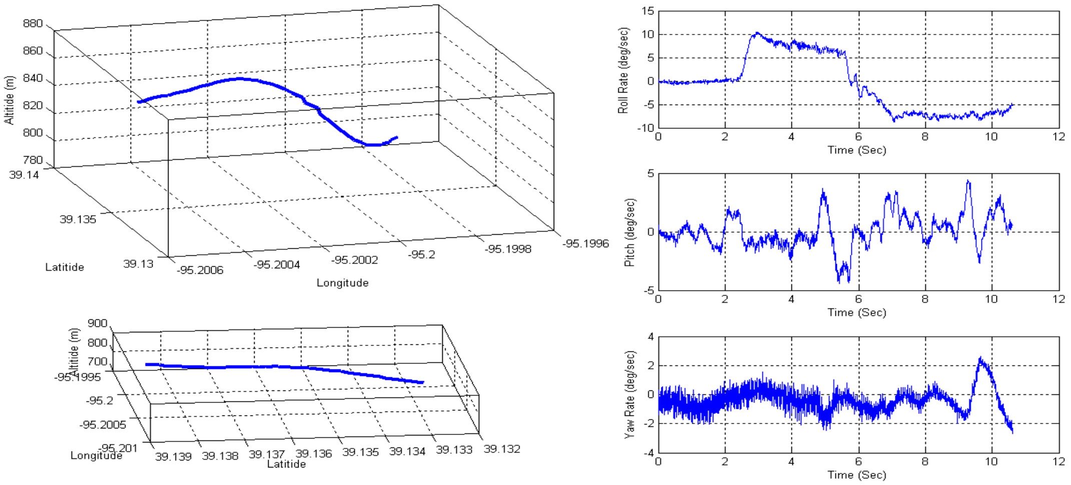


Figure B- 11: Short Impulses (Elevator Down)

Figures B-12 through B-15 show the flight track and MATLAB results during short duration impulse command to the rudder. At an IAS of 110 mph and 3000ft altitude the pilot commanded approximately 15% of the maximum rudder deflection for 1 second and allowed the airplane to settle before the next maneuver.

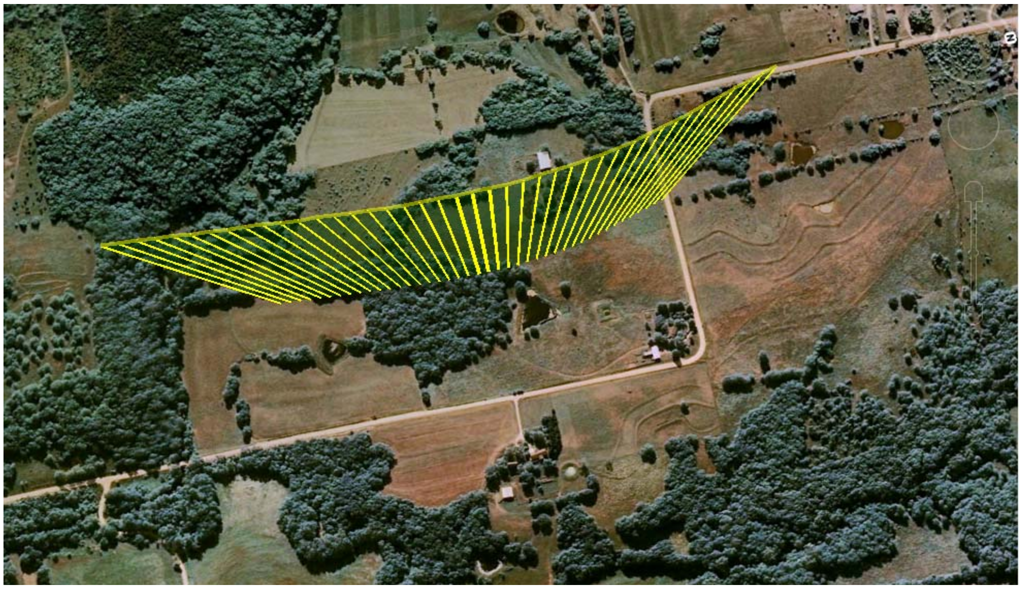


Figure B- 12: Google Earth Screenshot of Short Impulses (Rudder Left)

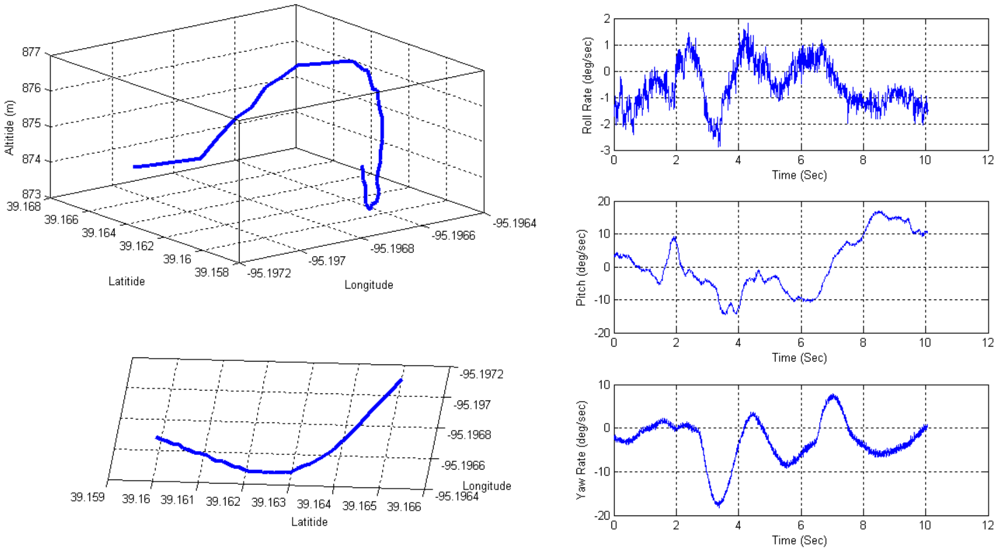


Figure B- 13: Short Impulses (Rudder Left)

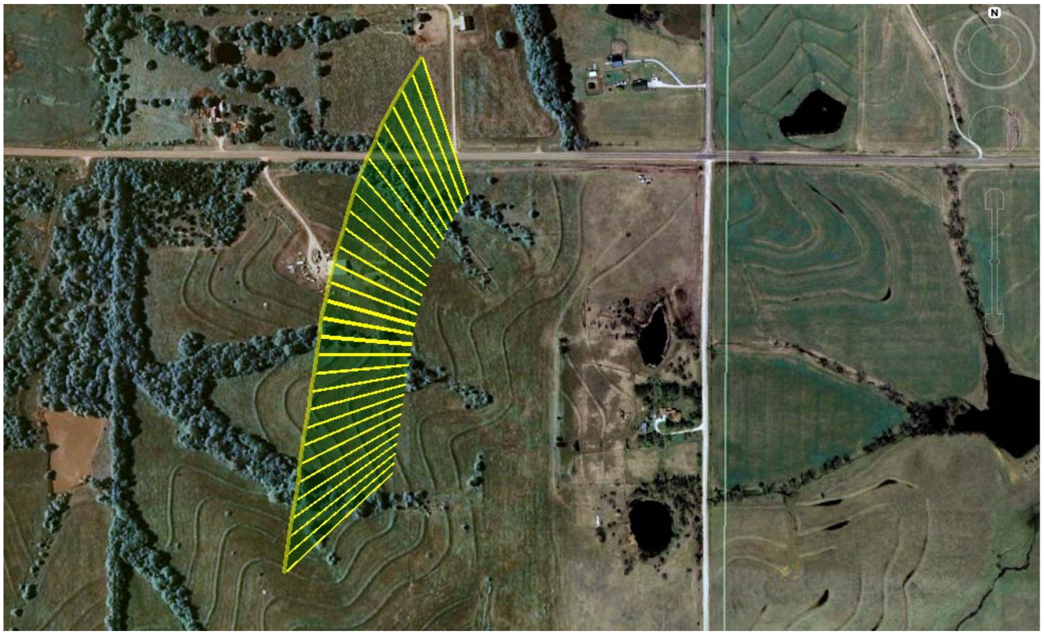


Figure B- 14: Google Earth Screenshot of Short Impulses (Rudder Right)

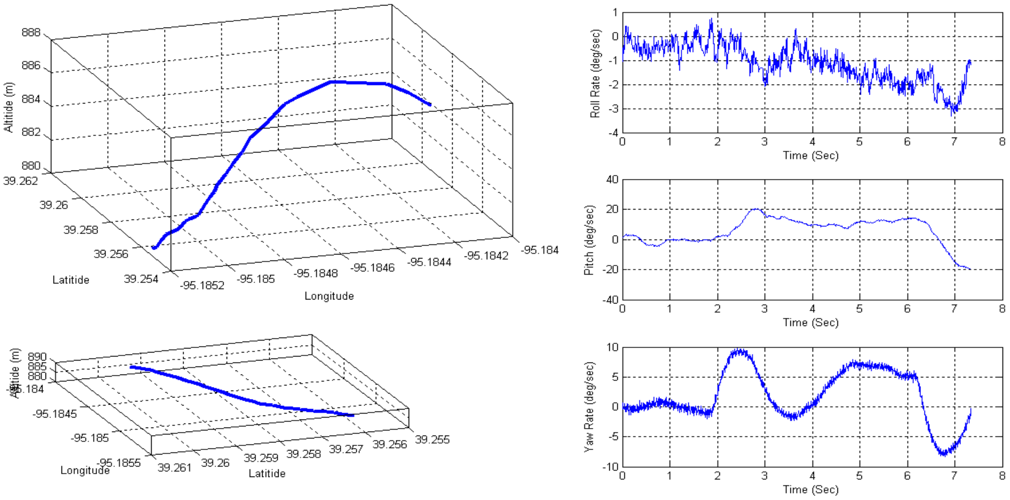


Figure B- 15: Short Impulses (Rudder Right)

Figures B-16 through B-19 show the flight track and MATLAB results during short duration impulse command to the aileron. At an IAS of 110 mph and 3000 ft altitude the pilot commanded approximately 15% of the maximum aileron deflection for 1 second and allowed the airplane to settle before the next maneuver.

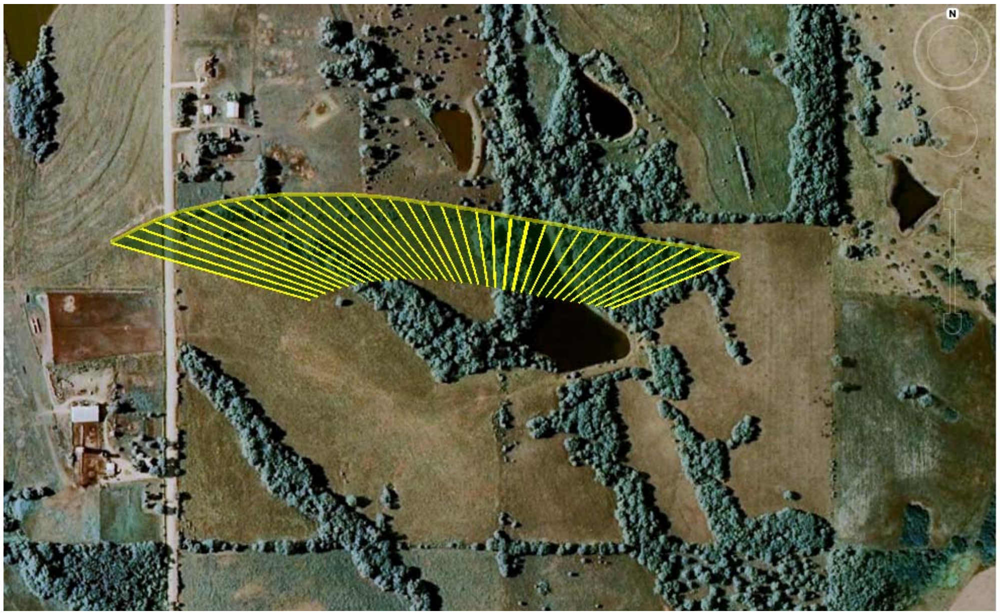


Figure B- 16: Google Earth Screenshot of Short Impulses (Aileron Up)

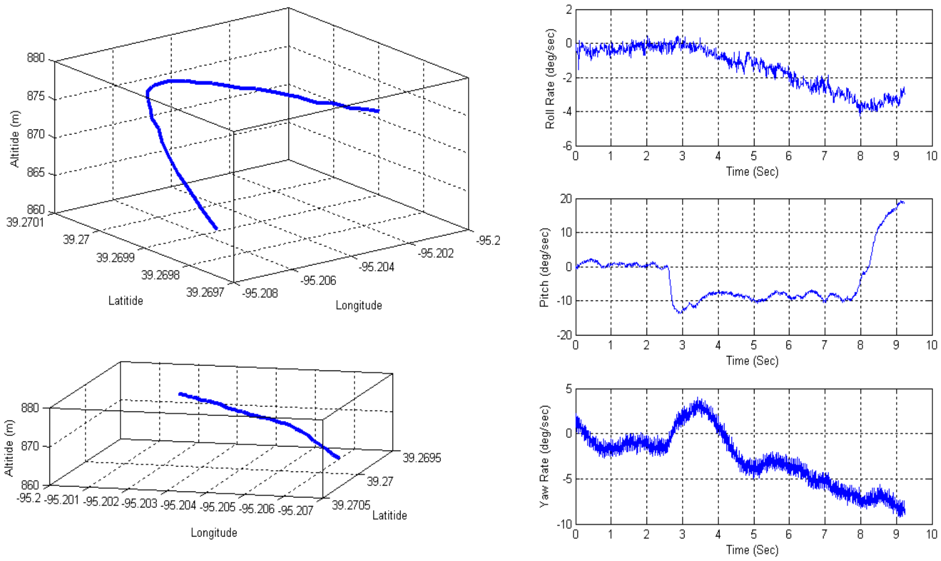


Figure B- 17: Short Impulses (Aileron Up)

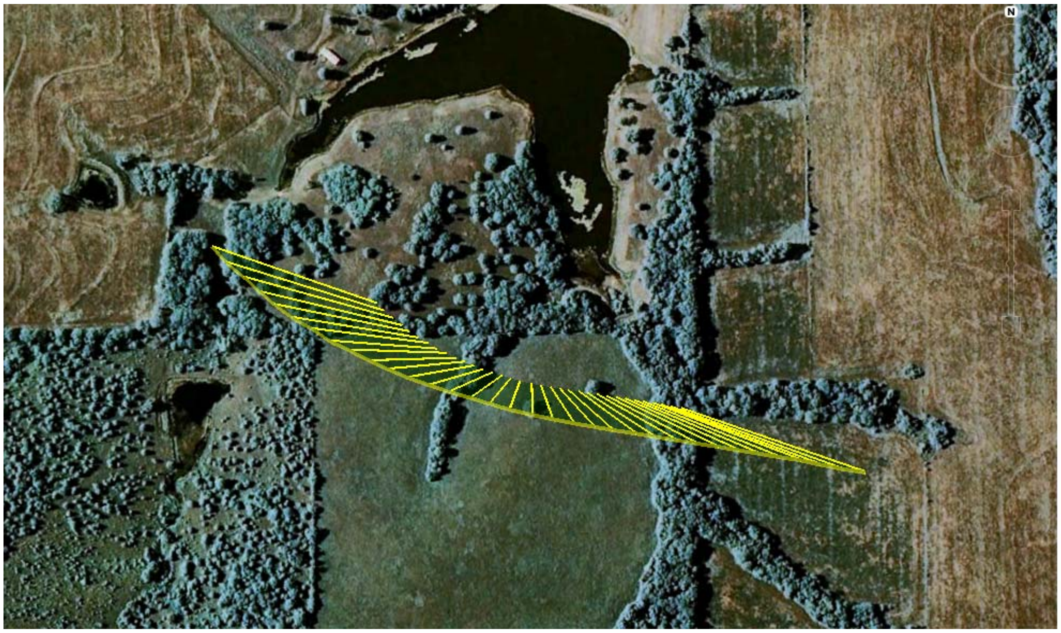


Figure B- 18: Google Earth Screenshot of Short Impulses (Aileron Down)

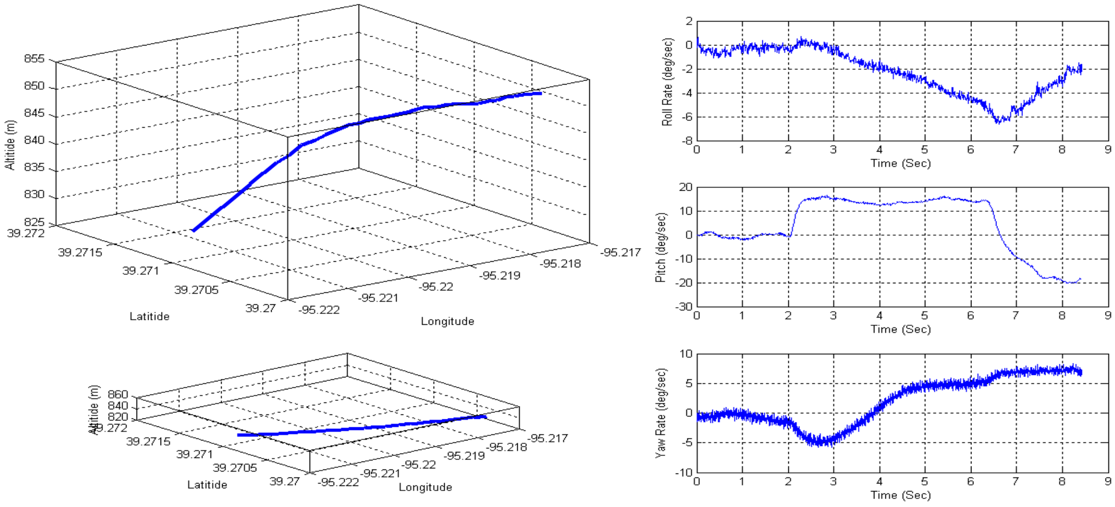


Figure B- 19: Short Impulses (Aileron Down)

Figure B-20 and Figure B-21 show, respectively, the flight track and MATLAB results from an elevator doublet. At an IAS of 110 mph and 3000 ft altitude, the pilot commanded approximately 25% of the maximum elevator deflection for 2 seconds up, followed by 2 seconds down with a return to center. Figure B-22 and Figure B-23 show the maneuver in which the deflection was for 2 seconds down, followed by 2 seconds up with a return to center.

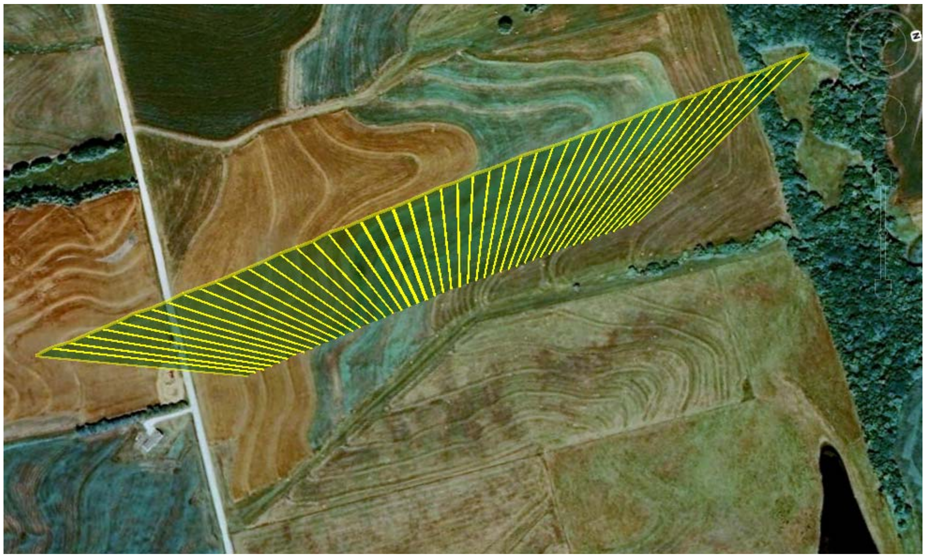


Figure B- 20: Google Earth Screenshot of Elevator Doublet (Up-Down-Center)

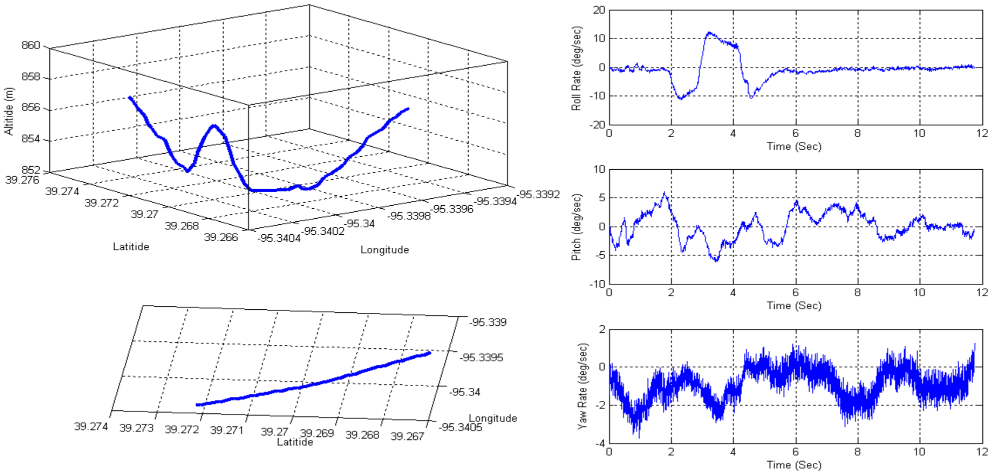


Figure B- 21: Elevator Doublet (Up-Down-Center)

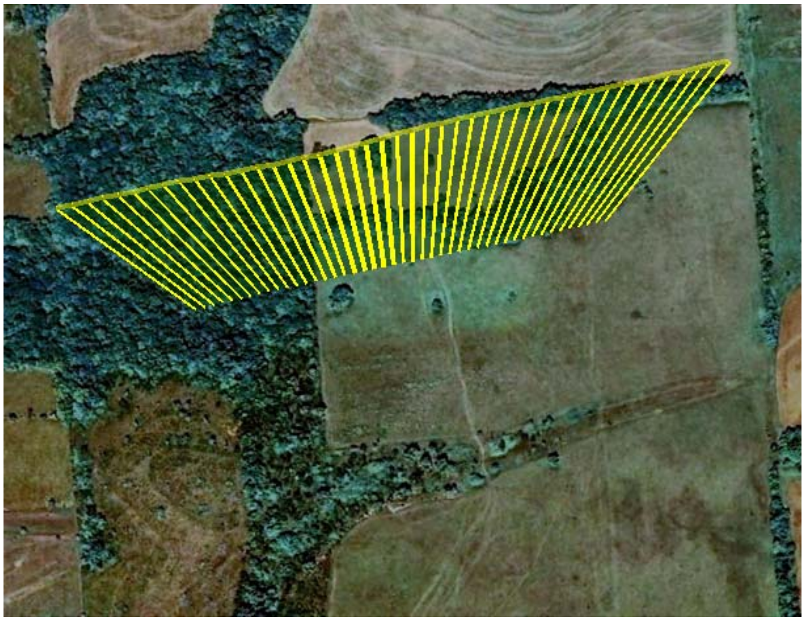


Figure B- 22: Google Earth Screenshot of Elevator Doublet (Down-Up-Center)

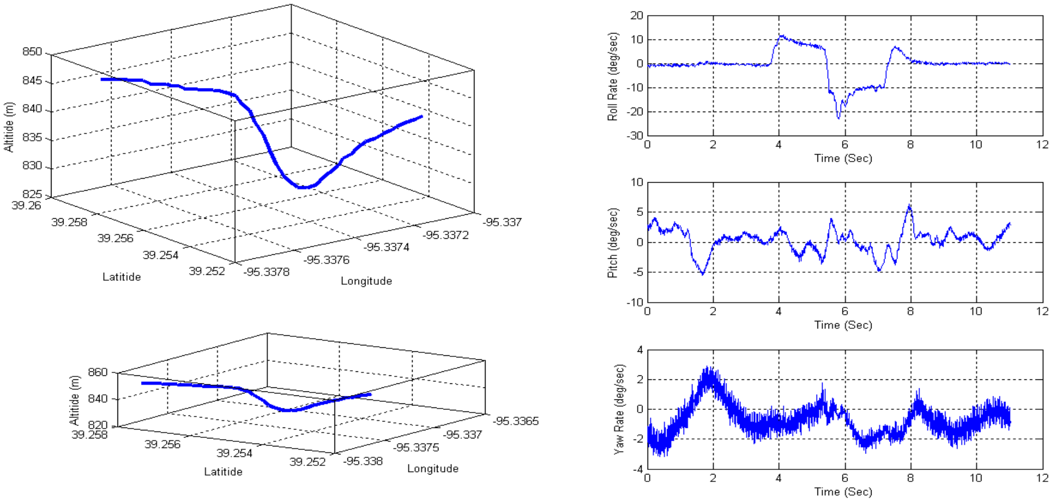


Figure B- 23: Elevator Doublet (Down-Up-Center)

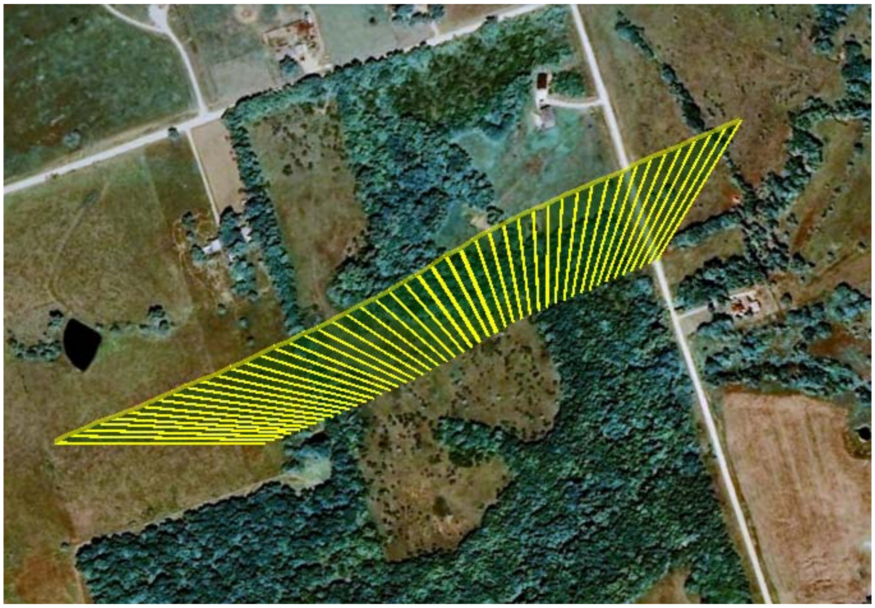


Figure B- 24: Google Earth Screenshot of Rudder Doublet (Left-Right-Center)

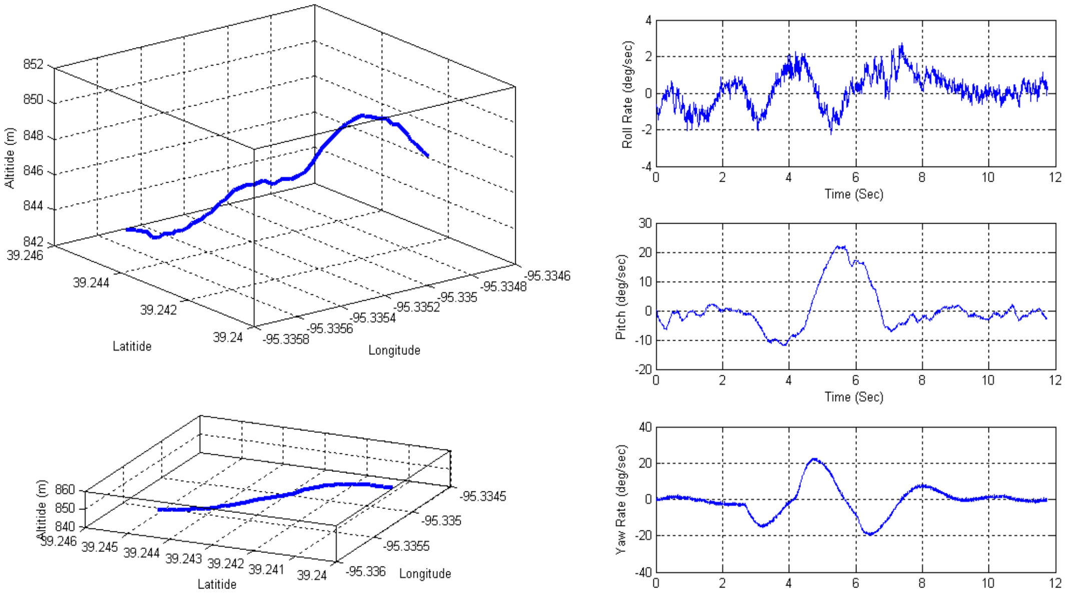


Figure B- 25: Rudder Doublet (Left-Right-Center)

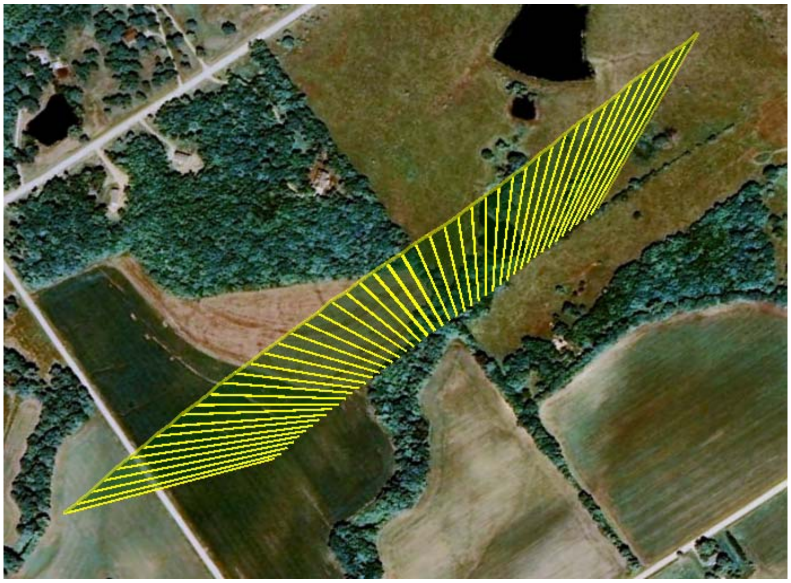


Figure B- 26: Google Earth Screenshot of Rudder Doublet (Right-Left-Center)

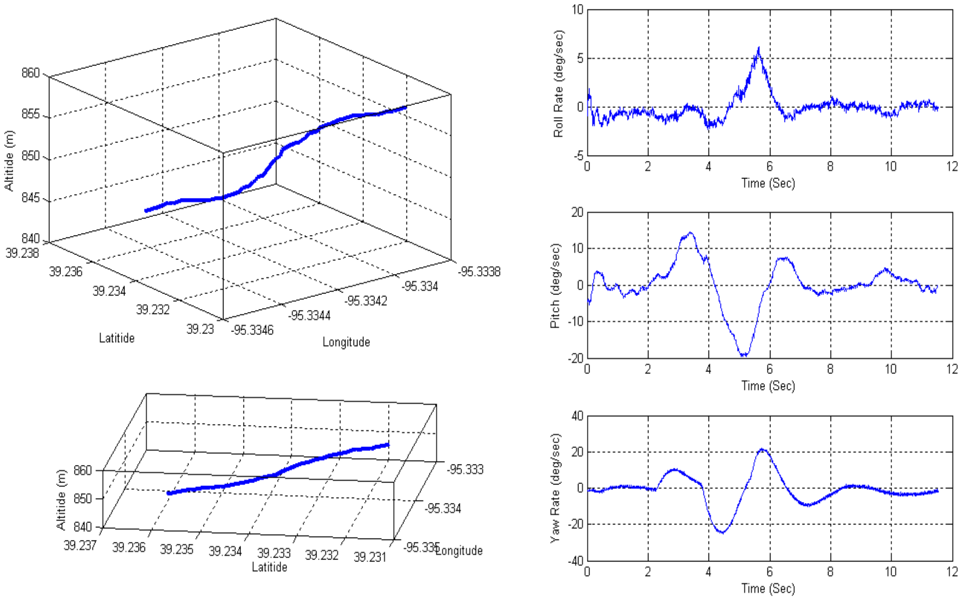


Figure B- 27: Rudder Doublet (Right-Left-Center)

Figures B-24 and B-25 show the flight track and MATLAB results from rudder doublet. At an IAS of 110 mph and 3000 ft altitude, the pilot commanded approximately 25% of the maximum rudder deflection for 2 seconds left, followed by 2 seconds right with a return to the center. Figure B-26 shows the maneuver in which the deflection was for 2 seconds right, followed by 2 seconds left with a return to center.

Figures B-28 and B-29 show the flight track and MATLAB results from aileron doublet. At an IAS of 110 mph and 3000 ft altitude, the pilot commanded approximately 25% of the maximum aileron deflection for 2 seconds left, followed by 2 seconds right with a return to the center. Figure B-30 shows the maneuver in which the deflection was for 2 seconds right, followed by 2 seconds left with a return to center.

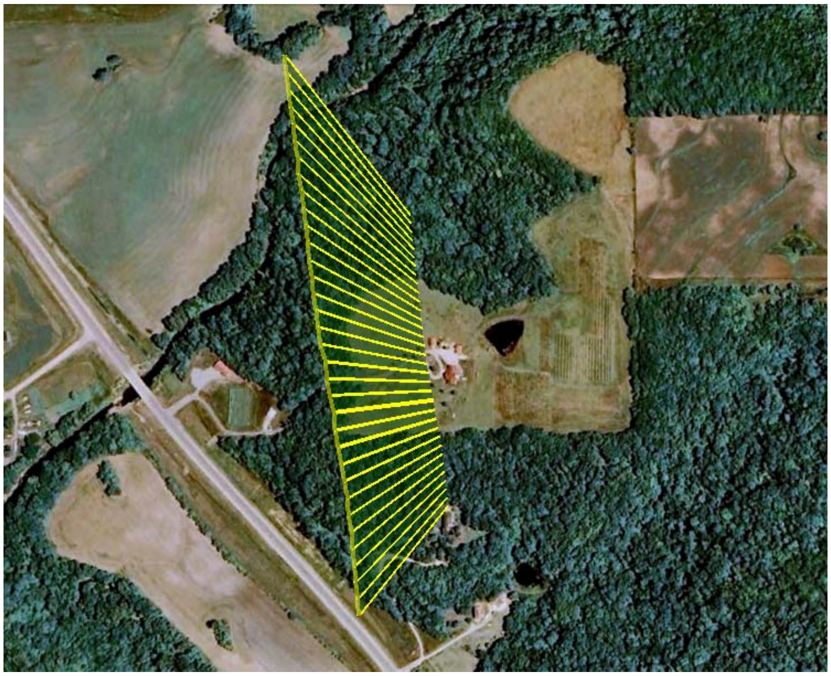


Figure B- 28: Google Earth Screenshot of Aileron Doublet (Left-Right-Center)

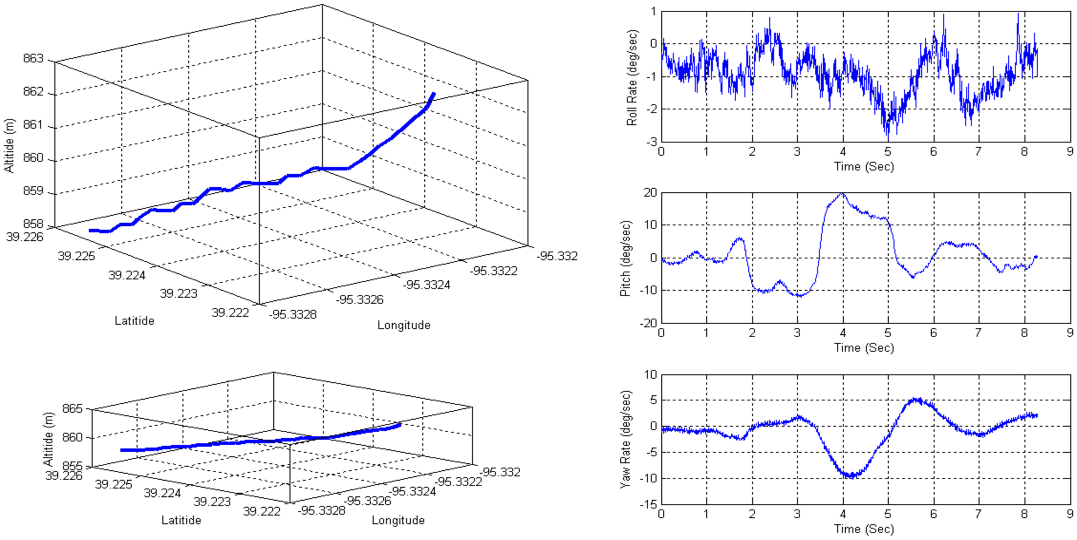


Figure B- 29: Aileron Doublet (Left-Right-Center)

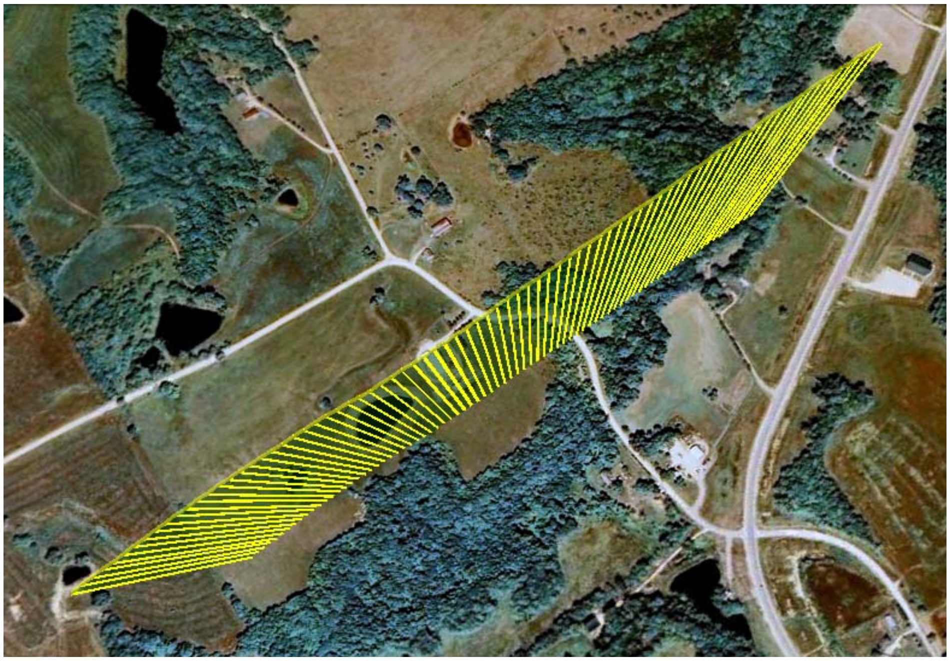


Figure B- 30: Google Earth Screenshot of Aileron Doublet (Left-Right-Center)

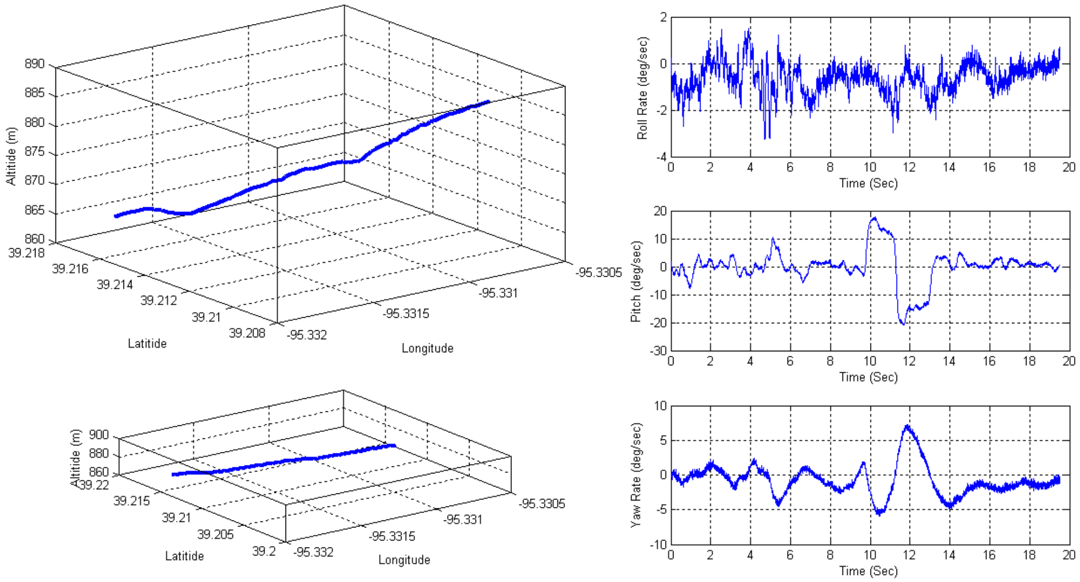


Figure B- 31: Aileron Doublet (Left-Right-Center)

Figure B-32 shows the flight track for a sideslip maneuver. At an altitude of 3000 ft and 110 mph IAS, a wings level sideslip of 5 degree sideslip angle to the left and then to the right was generated by holding first a left then a right rudder. The maneuver was then repeated for a steady heading sideslip by commanding the left rudder and then the right rudder for a 5 degree sideslip angle, all the while using a roll command as required. Figure B-33 through Figure B-36 give the MATLAB plots for the maneuvers.

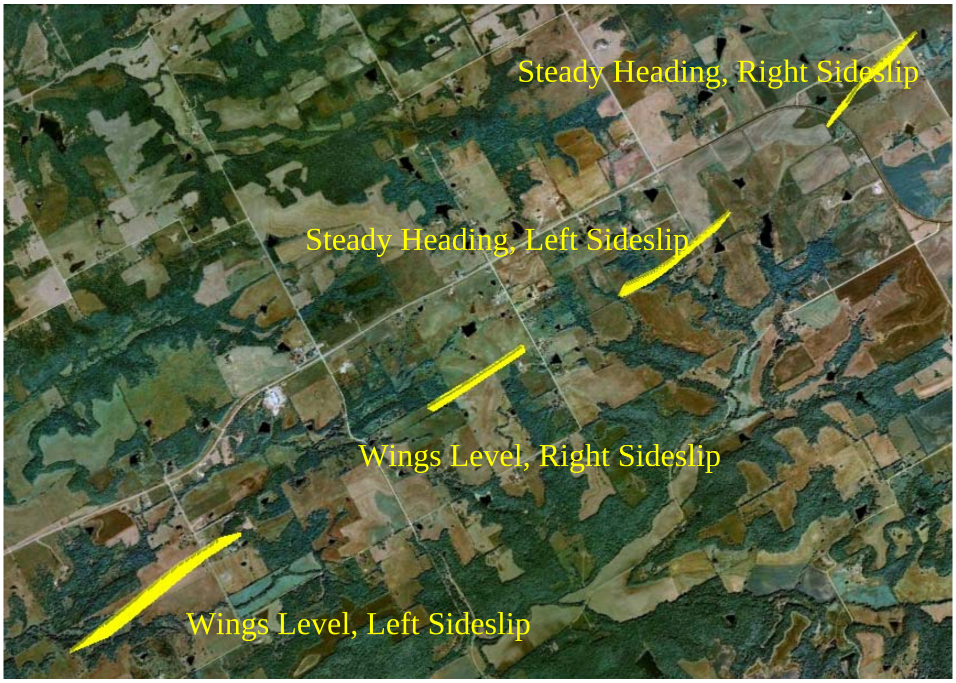

Steady Heading, Right Sideslip
Steady Heading, Left Sideslip
Wings Level, Right Sideslip
Wings Level, Left Sideslip

Figure B- 32: Sideslip (Wings Level and Steady Heading, Left/Right)

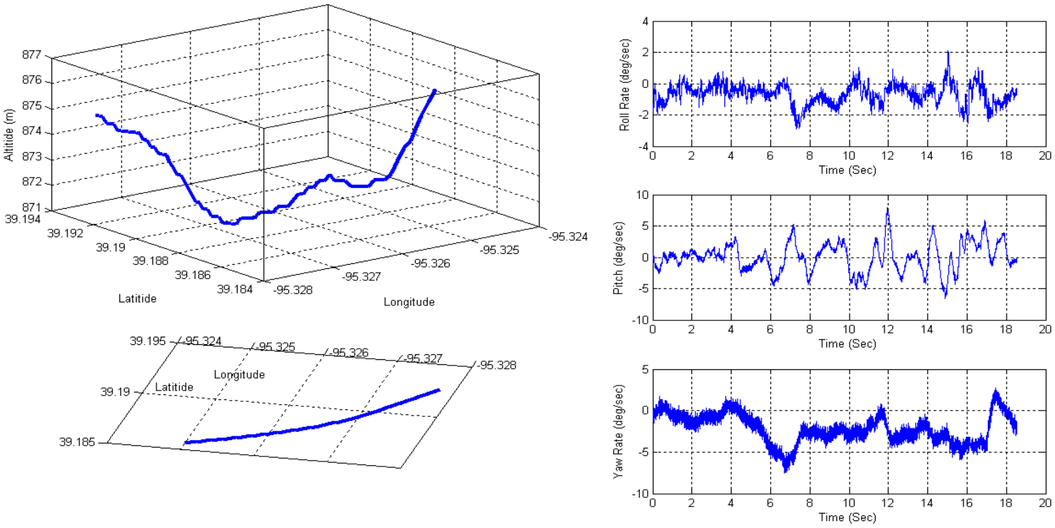


Figure B- 33: Left Sideslip (Wings Level)

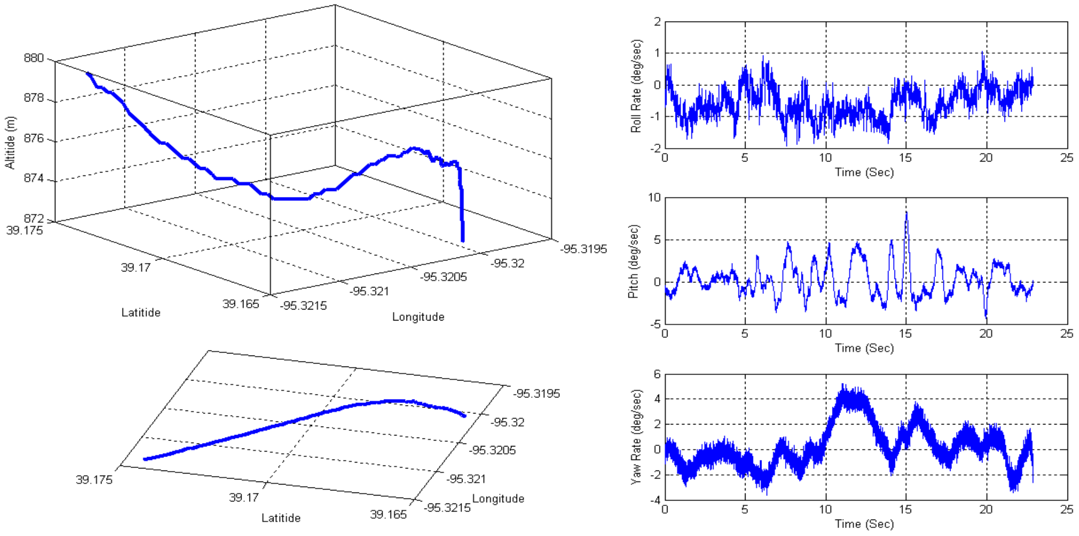


Figure B- 34: Right Sideslip (Wings Level)

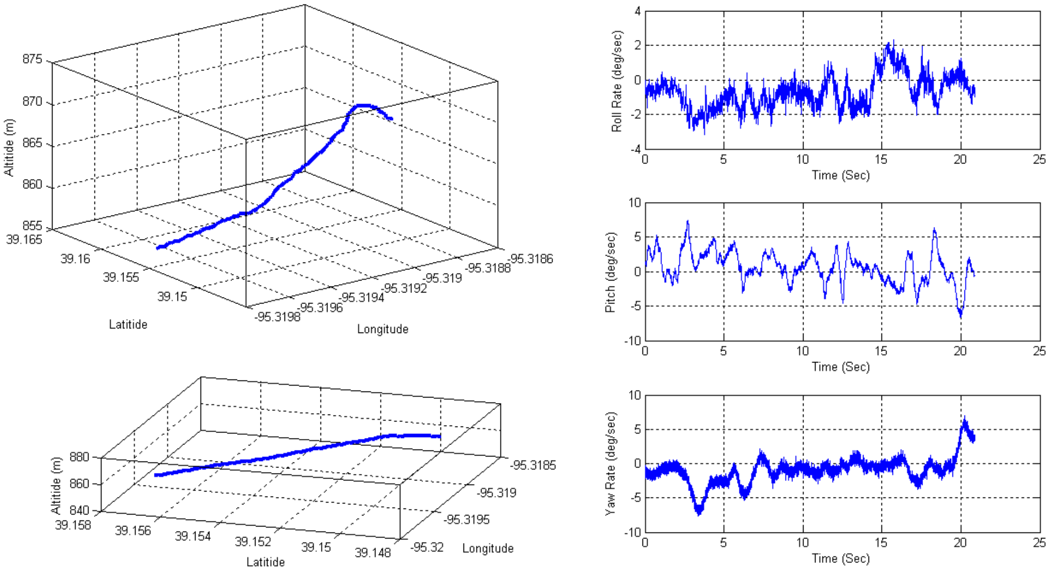


Figure B- 35: Left Sideslip (Steady Heading)

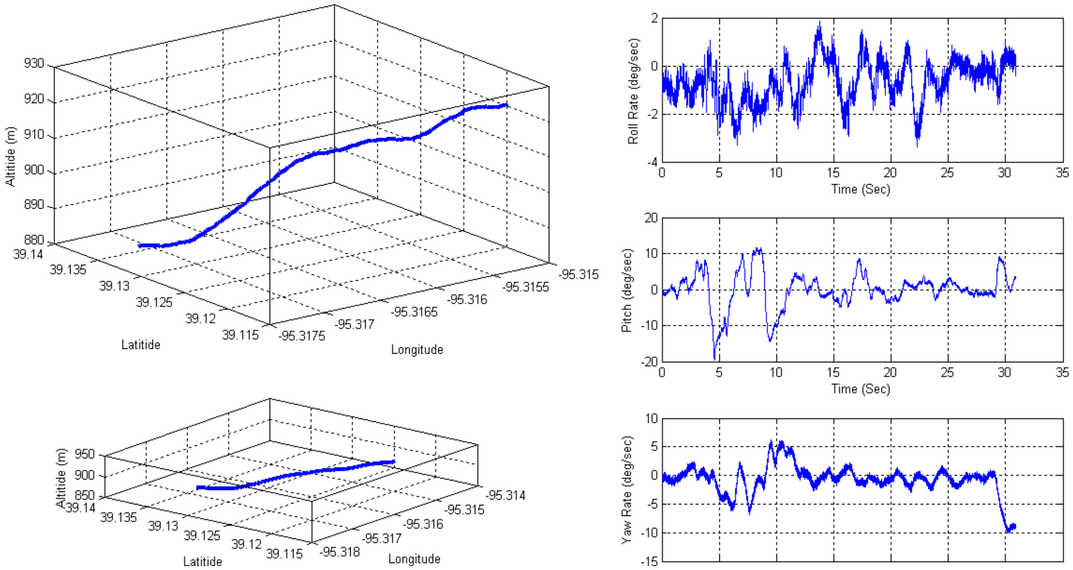


Figure B- 36: Right Sideslip (Steady Heading)

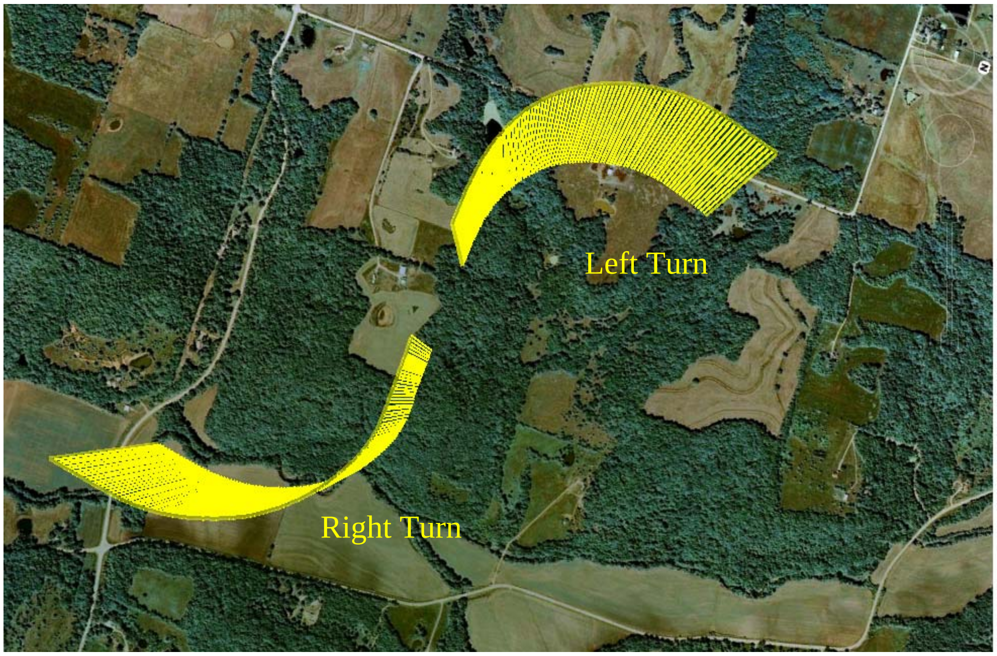


Figure B- 37: Google Earth Screenshot of Slow Flight Turn (Left/Right)

Figures B-37 shows the Google Earth screenshot for the slow flight turn to the left and then the right. The maneuver was performed at an altitude of 3000 ft and an IAS of 75 mph. The turn was performed at a bank angle of 20±5° through a turn of 90°. The break observed is due to the stopping of data logging and not due to loss of link. Figure B-38 and Figure B-39 are the plots obtained from MATLAB.

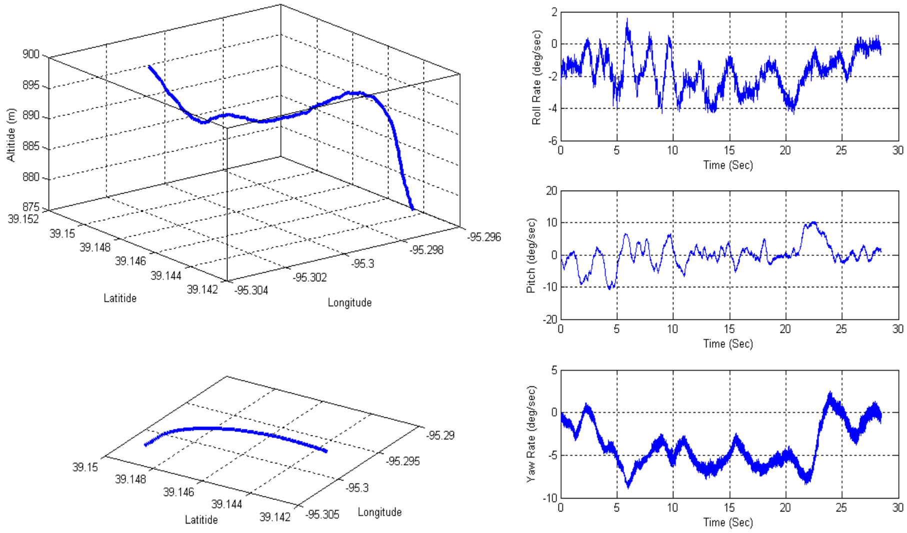


Figure B- 38: Slow Flight Turn (Left)

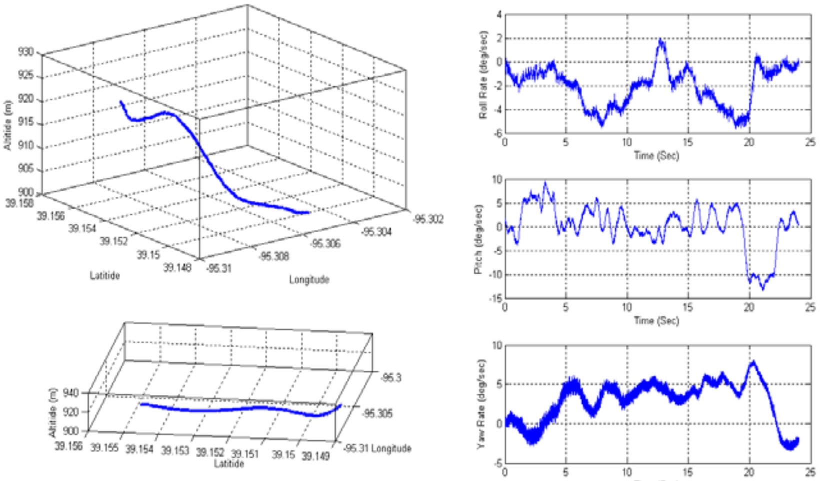


Figure B- 39: Slow Flight Turn (Right)

Figures B-40 through B-42 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 two sets – once for flap 10 and then continuously for flap 20, 30 and 40 degrees in a single file for the maneuver. The gap shown in Figure B-40 was due to the pause between the different flap settings. No packet losses were observed during this maneuver.

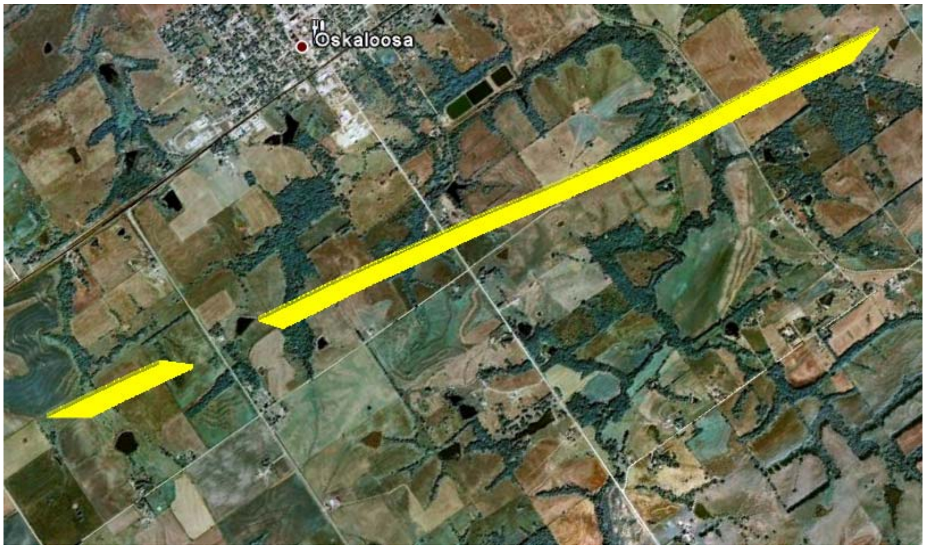


Figure B- 40: Google Earth Screenshot of Slow Flight with Varying Flap Settings

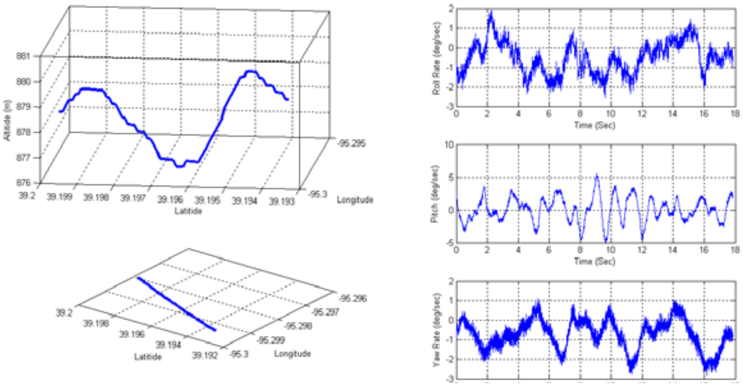


Figure B- 41: Slow Flight with 10 Degree Flap Settings

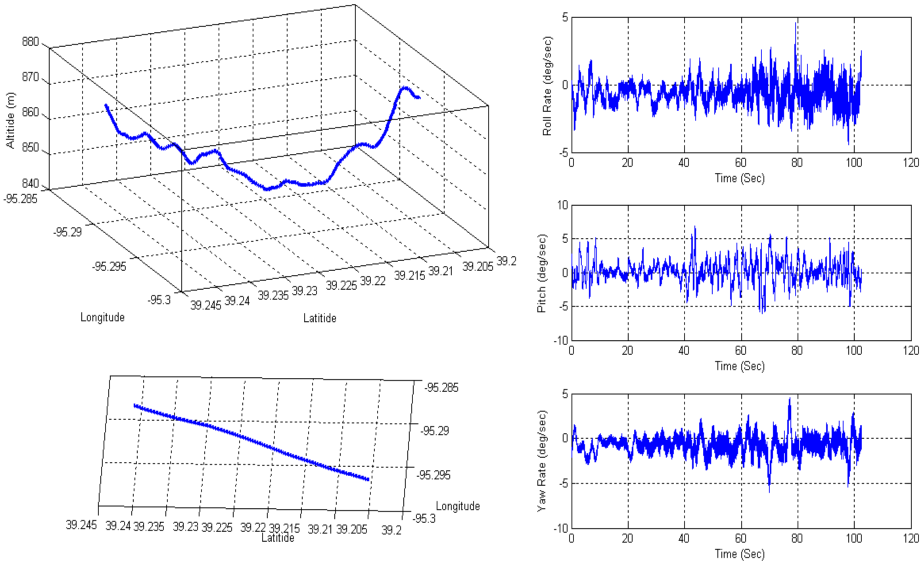


Figure B- 42: Slow Flight with Varying 20/30/40 Degree Flap Settings

Figures B-43 and B-44 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. No packet losses were observed during this maneuver.

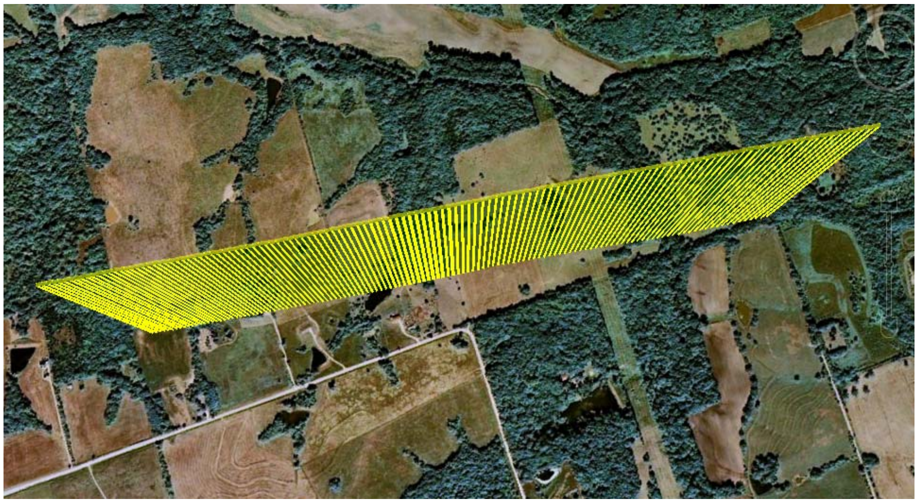


Figure B- 43: Google Earth Screenshot of the Accelerated Flight

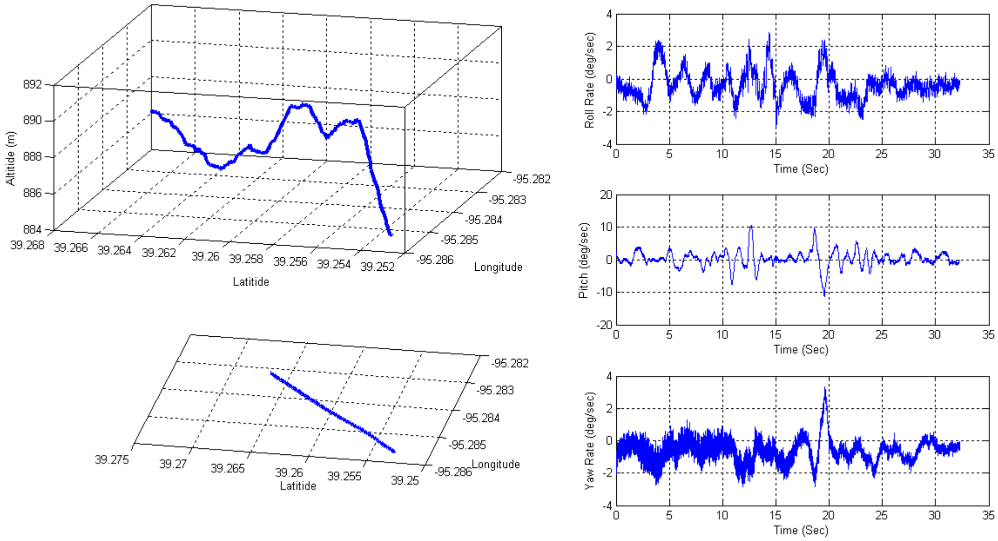


Figure B- 44: Accelerated Flight

Figures B-45 through B-48 show the flight track and the MATLAB plots during frequency sweep maneuvers of the 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 maneuver.

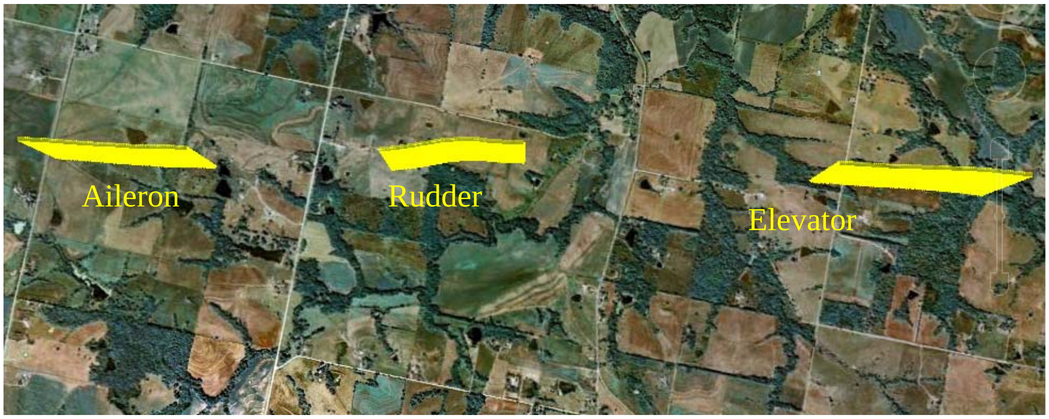


Figure B- 45: Frequency Sweeps (Elevator/Rudder/Aileron)

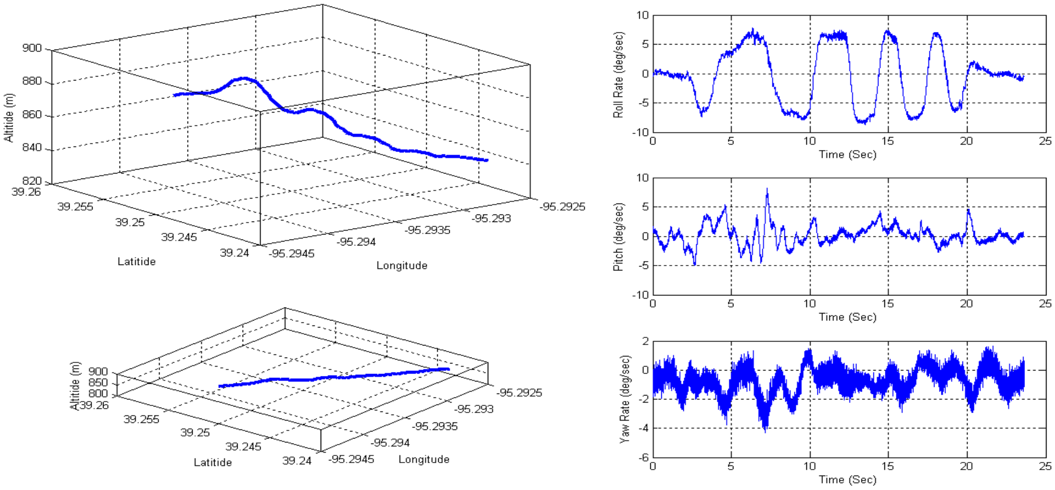


Figure B- 46: Frequency Sweep (Elevator)

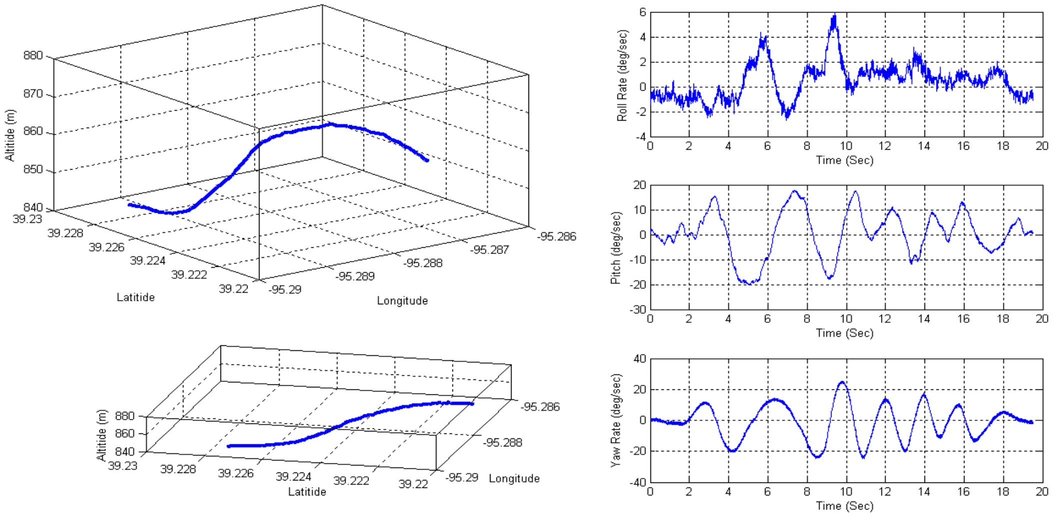


Figure B- 47: Frequency Sweep (Rudder)

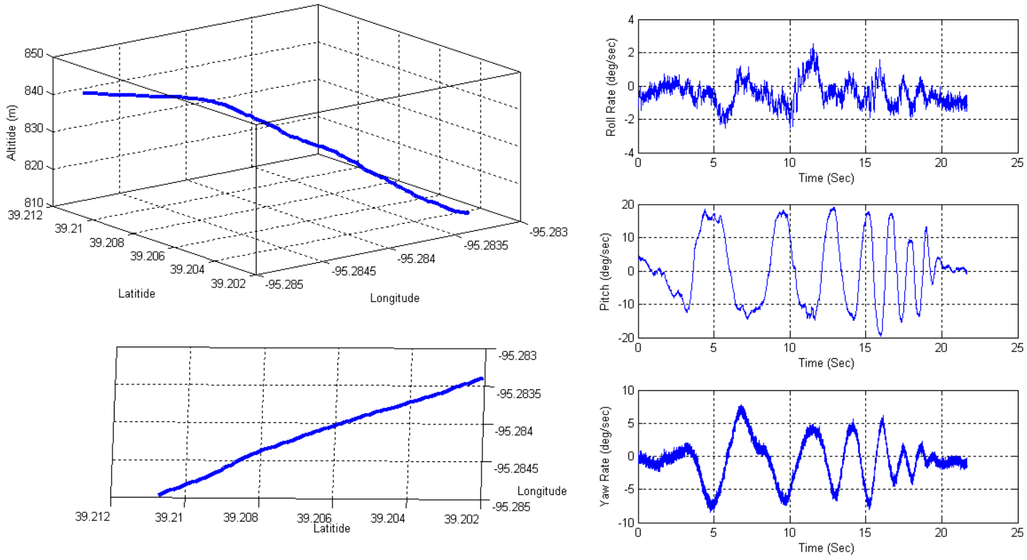


Figure B- 48: Frequency Sweep (Aileron)