

PERFORMANCE OF WIRELESS OFF-ROAD VEHICULAR NETWORKS

BY

TIMOTHY A WILCOX

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Agricultural Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2010

Urbana, Illinois

Master's Committee:

Professor Alan C. Hansen, Chair
Associate Professor Tony E. Grift
Assistant Professor Luis F. Rodríguez

ABSTRACT

Advances in wireless technology and an increasing demand for new applications that require in-field communication are generating more interest in off-road vehicular networks than ever before. Current on-road and off-road vehicular networking technologies are either cost prohibitive, bandwidth limited, or exhibit too much latency. 802.11 standard networks are a low-cost, readily available technology that have the potential of integrating effectively with current off road equipment software and hardware.

The main objective of this research was to develop a baseline for the performance of an 802.11b/g wireless network in a realistic in-field agricultural environment. While recognizing there are many external factors that can degrade the performance and reliability of such a system, this research was focused on identifying and measuring the performance effects of varying parameters that can be controlled, in particular the data rate, packet size, and the choice of 802.11b versus 802.11g protocols.

The performance of the system was measured by recording packets at both the transmitting and receiving devices and calculating the percentage of packets received at varying distances between the nodes. A simple two node network between two tractors was constructed for performance testing, and an application was written that used personal computers on each tractor to generate and log network traffic simultaneously. A series of 18 tests were executed with varying data rates, protocols, and packet sizes in realistic in-field conditions. Data were then post-processed so that they could be easily analyzed with the aid of Microsoft ExcelTM.

The 802.11b network performed much better in the outdoor environment by transmitting data more reliably and farther than the 802.11g network. 802.11g networks exhibited a high reliability region, usually at small distances between nodes, and a region with less reliability, at larger distances between nodes. Increasing 802.11g data rates decreased the distance over which the network would reliably transmit, but increasing 802.11b data rates had little effect on maximum transmission distance, although they decreased the overall reliability of the network. For packets between 15 and 1400 bytes in length, small but statistically significant decreases in reliability were observed with increasing packet size. For the largest packet size of 2200 bytes, more notable reliability decreases were observed. The network performance was influenced by

the angle of the transmitted wave relative to the tractor orientation. Finally, performance degradation due to signal reflections off the soil surface could be observed at distinct distances between nodes.

To Fred Nelson

"If I have seen further, it is only by standing on the shoulders of giants." – Sir Isaac Newton

ACKNOWLEDGMENTS

I extend my appreciation to Dr. Alan Hansen for his mentoring, assistance and guidance during my studies in the Agricultural Engineering Department and specifically during this work. Also thanks to Drs. Tony Grift and Luis Rodríguez for serving on my advisory committee and for providing helpful critique of this work.

Special thanks to John DeereTM for providing a portion of the equipment used in this work and for providing me with the flexibility to complete this research while working. Thank you to Jonathon McCrady for mentoring me while I completed my studies and research at the university, and to Robin Fonner for her eager willingness to help with the extra administrative burden required to complete this work after a leave of absence.

I would like to thank Greg and Linda Muehling for providing me with assistance collecting data for this work and support while completing my last semester of studies, including a place to stay and wonderful meals. Special thanks to Rachel Muehling for assistance proofreading and editing this work, and to Sky and Allison Sanborn for providing me with a place to stay in Champaign while finishing my degree.

I express my sincere gratitude to my family, Randy, Debbie, Jason and Andrew, for the lifelong love, support, and lessons they have instilled in me. Finally, I express my heartfelt love and appreciation to my wife, Rita, for her loving support, patience, and encouragement throughout my studies.

TABLE OF CONTENTS

LIST OF TABLES	vii
LIST OF FIGURES	viii
LIST OF ABBREVIATIONS.....	xii
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: OBJECTIVES AND SCOPE OF RESEARCH.....	4
CHAPTER 3: LITERATURE REVIEW	5
3.1 Open System Interconnection Model	5
3.2 Relevant Standards	6
3.3 802.11 Modulation Techniques	8
3.4 IEEE 802.11 History.....	11
3.5 Radio Propagation Fundamentals	14
3.6 Suitability of 802.11 in Vehicular Networks	25
3.7 Summary.....	26
CHAPTER 4: SYSTEM DESIGN AND VALIDATION	27
4.1 Hardware Setup.....	27
4.2 Hardware Configuration	30
4.3 Test Software Design and Implementation.....	31
4.4 Test Procedures.....	43
4.5 Summary	46
CHAPTER 5: RESULTS AND DISCUSSION.....	47
5.1 Ground Reflection Effects	47
5.2 Performance Differences Due to Orientation	52
5.3 Performance of 802.11b Versus 802.11g.....	56
5.4 Effect of Data Rate on 802.11 Reliability.....	58
5.5 Effect of Packets Size on 802.11 Reliability	61
CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS.....	64
REFERENCES	66
APPENDIX A: ENGENIUS™ 802.11 RADIO CONFIGURATION	71
APPENDIX B: IN-FIELD APPLICATION SOURCE CODE	76
APPENDIX C: PLOTS OF INDIVIDUAL RUNS	89

LIST OF TABLES

Table 1. Summary of Common Communications Protocols.	8
Table 2. Summary of 802.11 physical layer standards.	13
Table 3. Relative Advantages and Disadvantages of 802.11a, b, and g (Reproduced from Behzad, 2008).	13
Table 4. List of relative permittivity for common reflecting mediums (Lee, 1997).	17
Table 5. Sample Link Budget (Reproduced from Seybold, 2005).	24
Table 6. List of parameters and their descriptions in spatial output file.	41
Table 7. List of parameters and their descriptions in the statistical output file.	42
Table 8. Summary of runs displaying the various configurations tested.	44
Table 9. Distance between nodes where Fresnel radius equals antenna height for the first 10 Fresnel radii.	49
Table 10. Performance statistics comparing 802.11b and 802.11g networks.	58
Table 11. Maximum distance at which packets were received for the protocols tested.	59
Table 12. Results of two one-way ANOVA tests to determine if there were significant differences between packet sizes 1,2,3,4,5,6 and 1,2,3,4,5. The shaded regions denote analyses that are not statistically significant.	63

LIST OF FIGURES

Figure 1. IEEE 802.11 Chipset Volumes Through 2007 (Behzad, 2008).	3
Figure 2. The OSI network model showing data path between two nodes (Stallings, 1987).....	6
Figure 3. Representative FHSS hopping sequence for two node system (Olexa, 2005).	9
Figure 4. Formation of a DSSS waveform (Olexa, 2005).	10
Figure 5. Typical 802.11 OFDM channel showing subcarriers and spectral mask (Behzad, 2008).....	11
Figure 6. Diagram showing incident wave, reflected wave, transmitted wave, and grazing angle (Lee, 1997).....	16
Figure 7. Reflection coefficient versus grazing angle for both magnetic and electric portions of a wave (modified from Seybold, 2005).....	18
Figure 8. Diagram showing incident, reflected and direct waves (Rappaport, 2002).	18
Figure 9. Illustration of multipath signals distorting the original transmitted signal (Olexa, 2005).....	20
Figure 10. Schematic representation of Fresnel Ellipsoids (modified from Sizun, 2005).....	21
Figure 11. Diffraction and reflection signal attenuation and their relationship to Fresnel zone clearance (Lathi, 1965).....	22
Figure 12. Two tractors fitted with GPS hardware and radios for field tests.	28
Figure 13. GPS and radio mounted on a tractor showing the layout of the units.	29
Figure 14. System architectural diagram for test setup showing 802.11 radio network and supporting hardware.	30
Figure 15. Network diagram of test setup.....	31
Figure 16. Flow of data through data collection, post-processing, and analysis processes.	32
Figure 17. Flow diagram of in-field application software	34
Figure 18. Illustration of sequential packet transmission with length, L , and sequence number, SN	36
Figure 19. Picture of in-field application user interface displaying instantaneous and cumulative number of packets received for each packet length.....	37
Figure 20. Flowchart of post-processing application.....	39

Figure 21. Illustration of post-processing application function.	40
Figure 22. Normal path driven by two tractors during a data collection run.	45
Figure 23. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 5).	48
Figure 24. Plot of signal attenuation/amplification versus distance for antenna heights of 3.47 m and 4.00 m.	50
Figure 25. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 13).	51
Figure 26. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters illustrating the performance difference between nodes moving closer (Inbound) to each other versus farther away (Outbound).	53
Figure 27. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters illustrating the performance difference between nodes moving closer (Inbound) to each other versus farther away (Outbound).	53
Figure 28. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters using a modified driving pattern where illustrating the similarity in performance between nodes moving closer (Inbound) to each other versus farther away (Outbound).	55
Figure 29. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and 802.11b at 5.5 Mbits/sec and an antenna height of 3.47 meters (Runs 3 and 8).	56
Figure 30. Plot of reliability budget versus distance using 802.11g at 6 Mbits/sec and 802.11b at 5.5 Mbits/sec and an antenna height of 3.47 meters (Runs 3 and 8).	58
Figure 31. Plot of reliability budget versus distance for all 802.11b data rates using an antenna height of 3.47 meters.	60
Figure 32. Plot of reliability budget versus distance for all 802.11g data rates using an antenna height of 3.47 meters.	60
Figure 33. Plot of packets received versus distance using 802.11g at 18 Mbits/sec with an antenna height of 3.47 meters for all tested packet sizes (Run 5).	61
Figure 34. Operation mode setup for Engenius™ 802.11 radio.	71
Figure 35. LAN interface setup for Engenius™ 802.11 radio.	71
Figure 36. Basic wireless settings for 802.11 radio configured as access point.	72
Figure 37. Advanced wireless settings for 802.11 radio configured as access point.	73

Figure 38. Basic wireless settings for 802.11 radio configured as bridge.	74
Figure 39. Advanced wireless settings for 802.11 radio configured as bridge.....	75
Figure 40. Plot of packets received versus distance using 802.11b at 1 Mbit/sec and antenna height of 3.47 meters (Run 1).....	89
Figure 41. Plot of packets received versus distance using 802.11b at 2 Mbits/sec and antenna height of 3.47 meters (Run 2).....	89
Figure 42. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 3).....	90
Figure 43. Plot of packets received versus distance using 802.11g at 12 Mbits/sec and antenna height of 3.47 meters (Run 4).	90
Figure 44. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 5).	91
Figure 45. Plot of packets received versus distance using 802.11g at 36 Mbits/sec and antenna height of 3.47 meters (Run 6).	91
Figure 46. Plot of packets received versus distance using 802.11g at 54 Mbits/sec and antenna height of 3.47 meters (Run 7).	92
Figure 47. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 8).	92
Figure 48. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 9). Tractors drove back to starting position in reverse.	93
Figure 49. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 10).	93
Figure 50. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 11).....	94
Figure 51. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 12). Tractors drove back to starting position in reverse.....	94
Figure 52. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 13).	95
Figure 53. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 14). Tractors drove back to starting position in reverse.	95

Figure 54. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 4.00 meters (Run 15). Tractors drove back to starting position in reverse.....	96
Figure 55. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 16).	96
Figure 56. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 17). One vehicle remained stationary while the second drove pattern A.	97
Figure 57. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 18). Radio configurations were swapped for this run.	97

LIST OF ABBREVIATIONS

ANOVA	Analysis of variance
CAN	Controller area network
CAT5	Category 5
CPU	Central Processing Unit
CSV	Comma separated value
DSSS	Direct sequence spread spectrum
EIRP	Equivalent isotropically radiated power
EM	Electromagnetic
FCC	Federal Communications Commission
FHSS	Frequency hopping spread spectrum
GPS	Global positioning systems
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LLC	Logical Link Control
MAC	Media Access Control
MIMO	Multiple-input multiple-output
NMEA	National Marine Electronics Association
OEM	Original equipment manufacturer
OFDM	Orthogonal frequency-division multiplexing
OSI	Open System Interconnection
PC	Personal computer
PHY	Physical
RAM	Random-access memory
RFC	Request for Comment
RTK	Real Time Kinematic
SDM	Spatial-division multiplexing
STBC	Space-time block code
TCP	Transmission Control Protocol
TE	Transverse Electric
TM	Transverse Magnetic
TxBF	Transmit beam forming
UDP	User Datagram Protocol
WAVE	Wireless access in vehicular environments
XOR	Exclusive disjunction

CHAPTER 1: INTRODUCTION

Advances in global positioning systems (GPS), wireless communications, and electronic technologies have led to several innovations that have increased the efficiency and productivity of farmers around the world. One well-recognized example of such an innovation is the use of GPS-enabled navigation. While many factors affect the extent to which GPS-enabled navigation can increase agricultural profits, it has been estimated that farms employing this technology should boost profits by at least \$30 / hectare (Griffin, 2009). Still, in situations where machine interaction is common, or for tasks where multiple machine operations are required, a vehicular network offers significant potential to improve performance.

Harvesting in the Midwestern part of the United States is an example of a system that relies heavily on machine interaction and coordination. One, two, even as many as ten or more combines may be serviced by as many tractors towing grain carts with the throughput of the harvesting system being determined by the slowest link in the chain of operations. One case study by Hansen et al. (2003) analyzed a harvesting operation involving two combines and one grain cart in a rectangular-shaped field. In this study, one of the two combines sat idle for almost 10% of the time largely because it was waiting for the grain cart. Yet in the same field, the grain cart sat idle 28% of the time. Communication between the combines and grain cart to improve field logistics was identified by Hansen et al.(2003) as an option for improving the overall efficiency of the harvesting operation. Other applications have been identified such as "leader-follower," where the combine controls the position of the tractor and grain cart during the unloading process (Reid, 2004). These applications were envisioned by Reid (2004) as a natural extension of the current GPS-enabled navigation with the addition of an in-field vehicular network.

There are many instances where the on-road industry, both automotive and trucking, has been leveraged for research and technology that can be applied to off-road applications. The topic of vehicular networking so far has been an exception. Most research initiatives in the on-road industry have focused on wireless technologies relating to in-cabin or "infotainment" networks (Carvalho, 2008; Lupini, 2010). These networks are designed to communicate wirelessly between devices within the vehicle's cabin and are not suitable for in-field

communications. Other products exist that use cellular and satellite-based communications, but these products are very similar to products already being offered in the off-road industry and are not suitable for reasons stated below.

Currently, there are two types of networks used in the off-road equipment area. The first is cellular or satellite-based fleet management and machine tracking networks such as John Deere's JDLink™, Caterpillar's Product Link™, Topcon's Tierra Asset Manager™, and Trimble's VisionLink™ (Deere and Company, 2010; Caterpillar, 2010; Topcon, 2010; Trimble, 2010). These networks currently do not have the bandwidth and have too much latency to support real-time in-field network communication. The second type of network is a Real Time Kinematic (RTK) network for GPS corrections. RTK networks are advertised to work at distances up to 20 kilometers and because of this requirement, generally use proprietary radios (Deere and Company, 2010). These proprietary radios are normally expensive and require custom software to interface with them.

Possible alternatives to using proprietary radios and networks are wireless Ethernet or IEEE802.11 standard networks (IEEE, 1997), which pose many advantages as wireless communication technologies. The first advantage is the close relationship between the IEEE802.11 and IEEE802.3 (Ethernet) standards (IEEE, 1985). These standards were written with the intent of making transitions between the two protocols as easy and as seamless as possible by interfacing with adjacent layers using the IEEE802.2 standard (IEEE, 1985). With the use of access points, both a wired and wireless network can be merged into a single network. As the on-vehicle network bandwidth requirements continue to increase for off-road vehicle networks, 802.3 networks are an attractive candidate to carry large amounts of time-insensitive data. It would then follow that using 802.11 would further simplify many hardware and software design aspects. Next, the large consumer adoption of products conforming to both 802.11 (Figure 1) and 802.3 standard protocols has driven the hardware cost down.

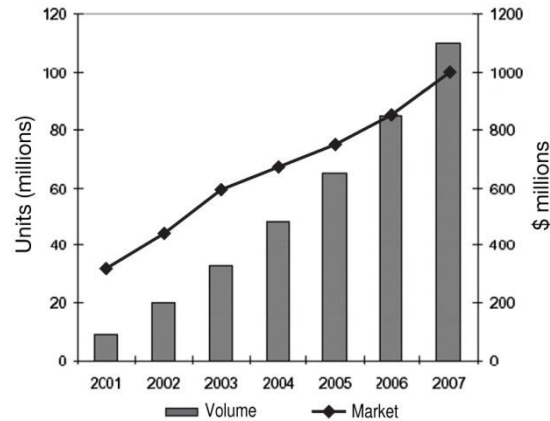


Figure 1. IEEE 802.11 Chipset Volumes Through 2007 (Behzad, 2008).

The industrial community has been increasingly using both 802.11 and 802.3, and as this demand increases, so does the availability and selection of durable networking hardware that could be used directly in the off-road vehicle environment (McCurdy, 2006; Warren, 2009). Lastly, both standards have been updated to stay current with new technology, but have provided legacy support for the widely used portions. Hardware meeting the IEEE802.3i standard from 1990 can still communicate over today's 802.3 networks due to legacy support provided in updates to the 802.3 standards (IEEE, 1990; IEEE, 1995; IEEE, 2008). Similarly, hardware meeting the 802.11b standard from 1999 is still compatible with current 802.11 wireless technology (IEEE, 1999; IEEE, 2003; IEEE, 2009). This long history of stable standards and backwards compatibility makes these technologies desirable for off-road equipment with longer life cycles.

In summary, recent advances in GPS technologies, electronics, and wireless communications have driven recent agricultural industry productivity and profitability improvements. In-field wireless networks combined with the aforementioned precision farming technologies enable the development of new applications that continue to fuel further improvements. Current on-road and off-road technologies are either cost prohibitive, bandwidth limited, or they exhibit too much latency. 802.11 standard networks are a low-cost, readily available technology that have the potential of integrating well with current off-road equipment software and hardware. This work serves to develop a baseline for the performance of an 802.11b/g wireless network in a realistic in-field agricultural environment.

CHAPTER 2: OBJECTIVES AND SCOPE OF RESEARCH

The primary objective of this research was to develop a baseline for the performance of an 802.11b/g wireless network in a realistic in-field agricultural environment. While recognizing there are many external factors that can degrade the performance and reliability of such a system, such as crop canopy, terrain, and line of sight issues, this research was focused on identifying and measuring the effects of varying parameters that can be controlled – in particular the data rate, packet size, and the choice of 802.11b versus 802.11g protocols.

The following were the specific goals addressed in the research:

- a) Establish a thorough understanding of the existing communication standards and protocols in the context of off-road application,
- b) Identify the key factors that could influence the performance and reliability of off-road wireless communication systems,
- c) Design and perform experiments to measure and evaluate an off-road wireless communication system.

The performance of the system was measured by recording packets at both the sending and receiving devices and calculating the percentage of packets received at varying distances between the nodes.

CHAPTER 3: LITERATURE REVIEW

This chapter contains a review of the literature relevant to this research. The first section establishes a general framework for networks, called the Open System Interconnection Model. The second section introduces the relevant protocols to this work, their standards, and their relationship to the Open System Interconnection Model. One of the key differences between the various 802.11 protocols is their modulation techniques, so section three explains the theory behind the modulation techniques before introducing the relevant 802.11 protocols in section four. Section five covers the fundamentals of radio wave propagation including sources of signal attenuation. Finally, section six discusses previous work aimed at evaluating the feasibility of 802.11 for vehicular networks.

3.1 Open System Interconnection Model

The Open System Interconnection (OSI) Model subdivides a network into smaller layers for the purpose of coordinating the development of standards and interfacing to the various portions of a network (ISO 7498-1, 1994). The OSI model is a seven-layered general model shown in Figure 2 which can be mapped to any kind of a layered network. Layers at the top of the model are usually embodied by an actual application, while layers at the bottom detail information relating to drivers or physical hardware. Figure 2 shows two nodes that are joined by a network with their representative OSI networking layers. The arrows represent the path a packet of data will travel along from one node to another.

When a packet of data needs to be transmitted over a particular network, it is initiated from one of the upper layers and travels in a downward direction between layers, each layer potentially adding its own information to the packet until it reaches the lowest layer, which is the physical transmission medium or hardware. Upon receipt at the receiving node, the data packet is then passed upward between the layers with each layer stripping off its own relevant data. The uppermost layer of the model is usually closest to the end user of the data, which can either be an application or a physical person operating a computer.

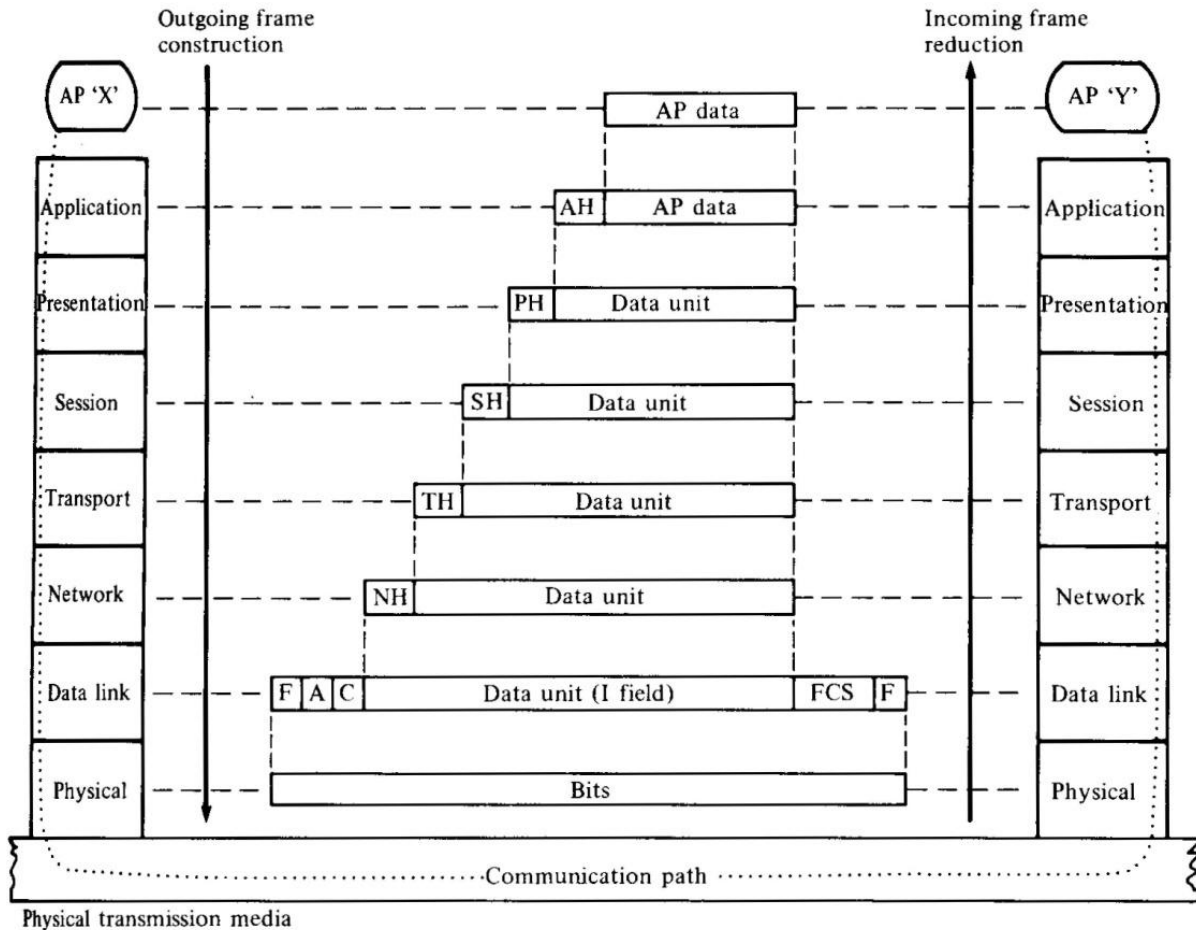


Figure 2. The OSI network model showing data path between two nodes (Stallings, 1987).

3.2 Relevant Standards

The IEEE 802 family of standards outlines the details of the physical and data link layers for multiple network topologies. Two of the most common types of networks that are defined by these standards are Ethernet (IEEE 802.3) and Wireless Ethernet (IEEE 802.11). The following details about these standards have been extracted from the most recently published versions of the standards and their amendments (IEEE, 1998; IEEE, 2008; IEEE, 2007). These two standards define the physical layer and a portion of the data link layer, which are referred to in the standards as the Physical (PHY) Layer and Media Access Control (MAC) Layer, respectively, as shown in Table 1. Both 802.11 and 802.3 share the same logic for linking the MAC layer to the network layer. This logic is defined in IEEE 802.2 and is commonly referred

to as the Logical Link Control (LLC) Layer. The common LLC layer between the two standards is what makes Ethernet and Wireless Ethernet networks seamlessly interchangeable and allows them to interact identically with data from the network layer. The data link layer is generally implemented in the device drivers or low level firmware of the physical transmitting device. For most practical situations, an application will interact with the operating system at the transport layer because there are features or services provided by the network and transport layers that are needed for effective network communication and function. Internet Protocol packets are a standard protocol used for the network layer and are defined by Request for Comment 791 (RFC 791, 1981). Internet Protocol (IP) packets contain an address that allows for the packet to be dynamically routed to its destination. This addressing system allows for flexible networks that can have their architecture changed easily. Another important capability that is introduced through IP packets is the ability to form sub-networks. The transport layer serves to take a large amount of data and break it into small transportable packets that can be sent across the network. At the receiving node, these individual packets are reassembled to identically reconstruct the original piece of data. There are many types of protocols that can be used in the transport layer. Two of the most popular are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP is a simple, lightweight protocol that is defined by RFC 768 (1980). TCP is more complex than UDP but offers the advantage of providing a notification of receipt of the original data at the expense of a less-efficient protocol. It is defined by RFC 793 (1981).

For the tests conducted in this research, packets were transmitted and received at the transport layer. Therefore, discussions relating to other layers above the transport layer are outside the scope of this work.

Table 1. Summary of Common Communications Protocols.

OSI Layer	Communications Protocol	Standard	
Transport	UDP or TCP	RFC 768 (UDP) or RFC 793 (TCP)	
Network	IP	RFC 791	
Data Link	LLC	IEEE 802.2	
	MAC		
Physical	PHY	IEEE 802.11	IEEE 802.3

3.3 802.11 Modulation Techniques

Three types of modulation techniques – frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and orthogonal frequency division multiplexing (OFDM) – are referenced in the 802.11 standards and amendments. FHSS and DSSS are types of spread spectrum techniques, which means the transmission signal is spread over a larger portion of the spectrum than what is required to transmit the data (Pickholtz et al., 1982). OFDM works by subdividing a channel into multiple subcarriers that carry portions of the data stream in parallel. A brief overview of these three techniques is provided in the following sections.

3.3.1 Frequency Hopping Spread Spectrum (FHSS)

FHSS systems place data in a narrow band but modulate that carrier frequency in a defined pattern often referred to as a code or hopping sequence (Figure 3). In order to make rapid and frequent changes to the carrier frequency, both the transmitting and receiving device must share the same code and be designed for rapid frequency changes. The transmitted signal is left unaltered other than to change the carrier frequency. By changing the carrier frequency, interference is averaged between channels instead of directly affecting one channel more than any other. FHSS systems are very common in military applications where a high immunity to signal jamming is required (Ipatov, 2005).

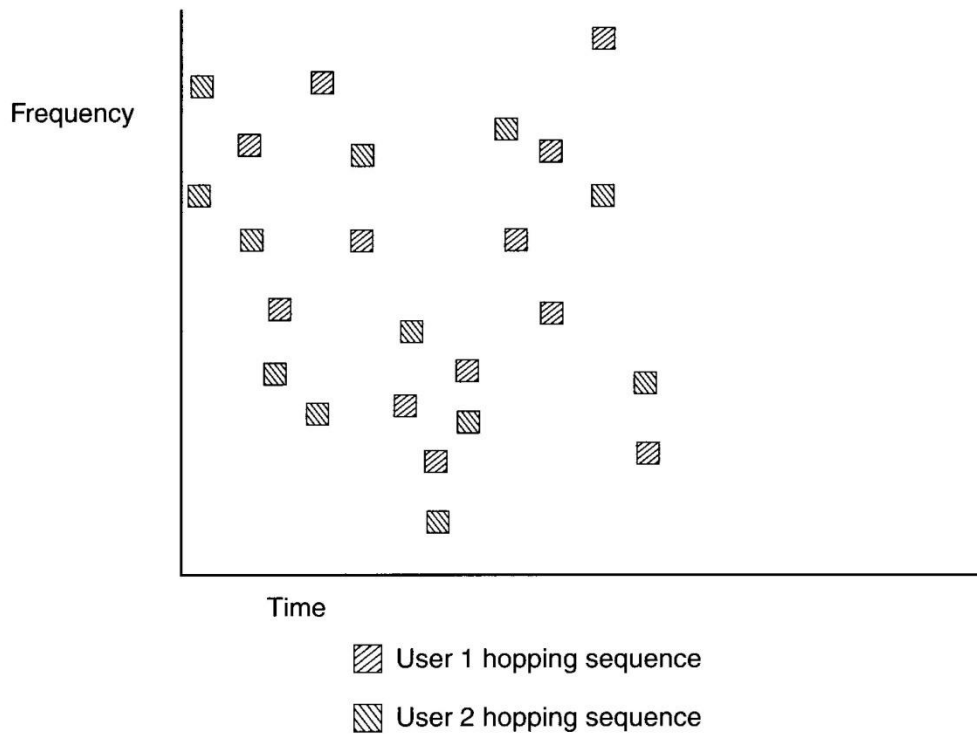


Figure 3. Representative FHSS hopping sequence for two node system (Olexa, 2005).

3.3.2 Direct Sequence Spread Spectrum (FHSS)

In contrast, DSSS systems spread the information signal or baseband signal about a fixed frequency carrier signal which has much wider bandwidth than the original signal (Figure 4). This is accomplished by taking the exclusive disjunction or XOR of the original signal with the spreading code. The transmitted DSSS waveform is usually spread across such a large frequency range that the resulting waveform is not distinguishable from the surrounding ambient noise. Encapsulating data in a wide frequency band also allows for narrow band interference to be easily rejected (Olexa, 2005). However, if the interference is at a high energy level, DSSS systems will completely fail (McCune, 2000). Lastly, since DSSS systems broadcast low amounts of energy over a wide range, they work better in situations where there are many users sharing the same portion of the spectrum.

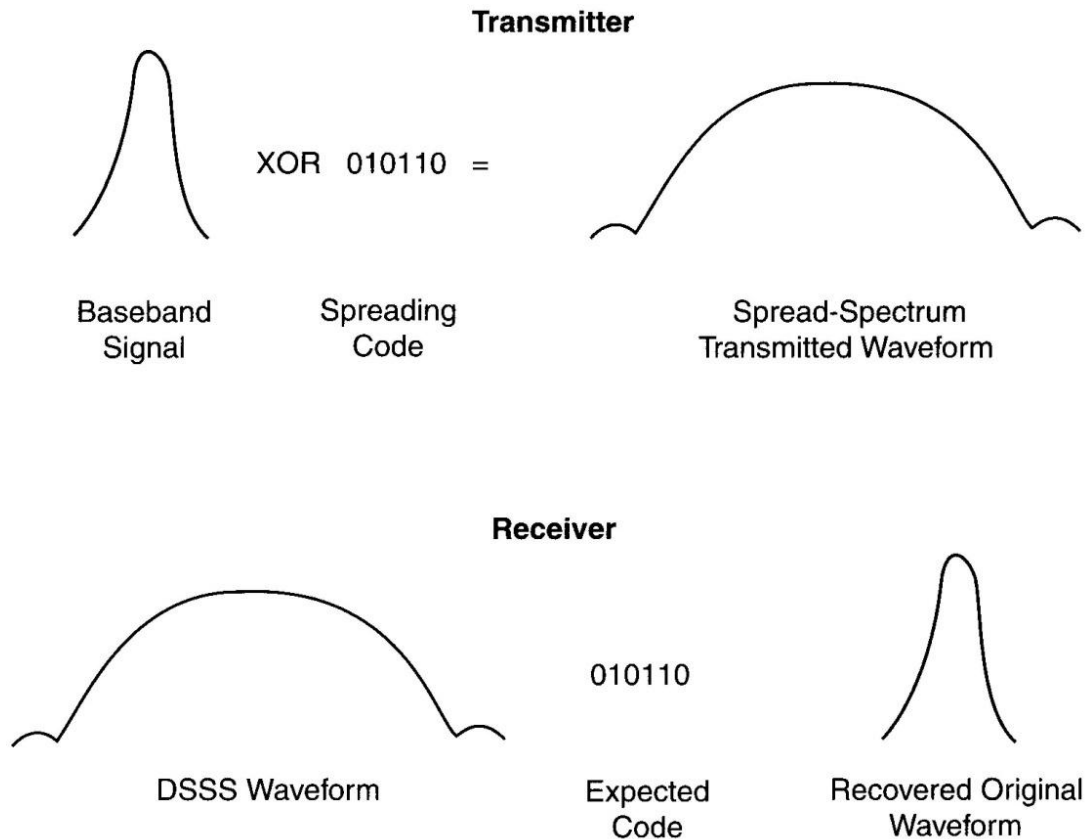


Figure 4. Formation of a DSSS waveform (Olexa, 2005).

3.3.3 Orthogonal Frequency Division Multiplexing (OFDM)

As the push for higher data rates continues, the performance of spread spectrum technologies degrades because all of the data are transmitted serially by the wireless signal. Because the data rate and symbol duration are inversely related in DSSS systems, the amount of spacing between each symbol decreases, and the probability of intersymbol interference increases (Li and Stüber, 2006). OFDM addresses this problem by dividing the channel into narrow subchannels or subcarriers which allow the data to be transmitted in parallel across the subchannels (Figure 5). Each subchannel is independently modulated by the radio, allowing for more flexibility to maximize throughput. For example, for a given propagation path, if a particular subcarrier encounters fading, the radio can assign a lower order modulation to maximize reliability for that subchannel. If other channels do not experience the same fading, they can be modulated at much higher order modulations to maximize throughput. The tradeoff for this extra flexibility is added complexity and hardware cost. Furthermore, OFDM radios are

susceptible to frequency drift, either caused by poorly performing hardware or external sources (Olexa, 2005). Olexa (2005) also states that OFDM radios have a high immunity to multipath distortion but are very susceptible to narrowband inference, but as discussed later, 802.11 systems using OFDM do not always outperform other 802.11 systems when multipath is present in outdoor environments (Alexander et al., 2007).

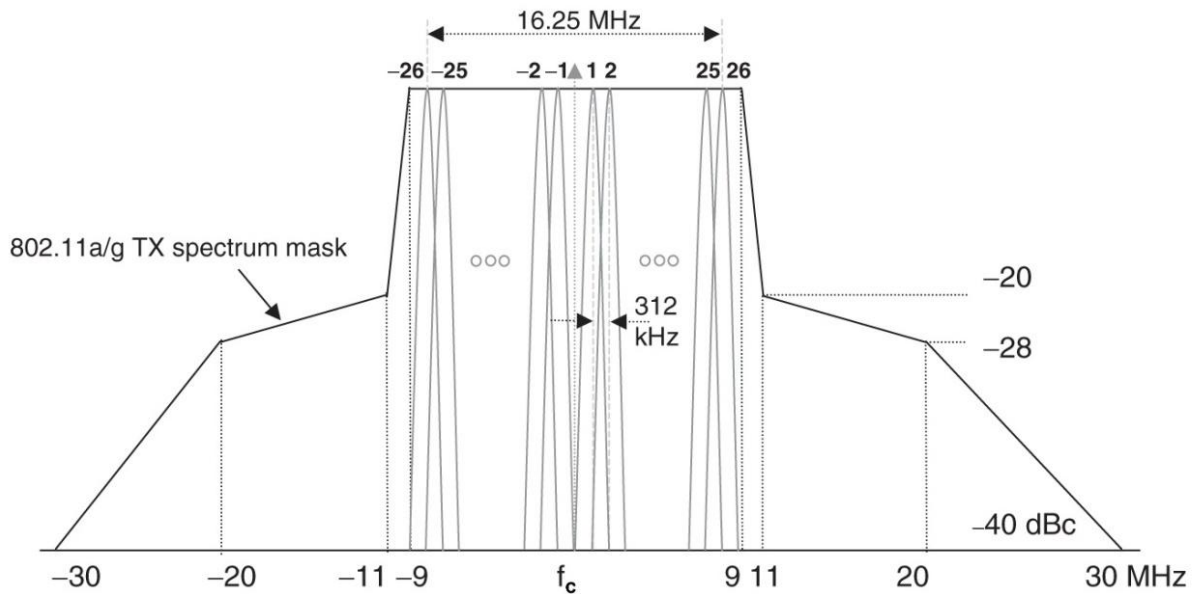


Figure 5. Typical 802.11 OFDM channel showing subcarriers and spectral mask (Behzad, 2008).

3.4 IEEE 802.11 History

The original IEEE 802.11 standard was ratified in 1997. This served as the base standard for 802.11 devices until it was replaced by the current base standard IEEE (2007). The original 802.11 standard defined the MAC layer for all 802.11 devices as well as three different physical layer options, which were an infrared physical layer, a FHSS 2.4 GHz layer, and a DSSS 2.4 GHz layer. The maximum data rate at the MAC layer for the standard was 2 Mbits/sec. In 1999, the base 802.11 standard was updated to make changes to the MAC layer, and two additional physical layer standards were ratified: IEEE 802.11a and IEEE 802.11b. 802.11a defined an OFDM physical layer operating in the 5.5 GHz unlicensed band to take advantage of the fact that

there is much less spectral competition and interference at the 5.5 GHz band than at the 2.4 GHz unlicensed band. The 802.11b standard expanded the functionality on the original 802.11 DSSS 2.4 GHz physical layer to allow for a maximum MAC data rate of 11 Mbits/sec while still maintaining compatibility with the DSSS portion of the original standard. 802.11b was regarded as the most successful 802.11 standard to date, selling millions of pieces of hardware complying with the standard (Heegard, 2001). In 2003, another physical layer specification called 802.11g was ratified that allowed for the use of the OFDM modulation techniques of the 802.11a standard to be used with a 2.4 GHz physical layer. This standard once again maintained compatibility and coexistence with 802.11b systems while allowing for the MAC data rate to be increased up to 54 Mbits/sec. In 2007, many of the amendments to the original 802.11 standard, including 802.11a, b, and g, were merged into a single base document named IEEE 802.11-2007 which is the current base standard. Table 2 summarizes the standards' properties and modulation techniques, and Table 3 compares the relative advantages and disadvantages of 802.11a, b, and g.

The amendments to the 802.11 standards previously mentioned had been narrow in scope, focusing on higher data rates and range while maintaining backwards compatibility with legacy standards. The scope of the IEEE802.11n was much larger. This amendment pushed the MAC layer throughput to 600 Mbits/sec by using an antenna technology called multiple-input multiple-output (MIMO), which allows multiple spatial streams to be transmitted and received by communicating devices. Additionally, to achieve a MAC layer throughput of 600 Mbits/sec, an increase in channel width from 20 MHz (Figure 5) to 40 MHz was required, allowing for more subchannels to be utilized. However, implementing MIMO technology physically takes more space, requires more power, and adds cost – three characteristics not sought by manufacturers of mobile handheld devices (Perahia, 2008). As a result, many of the features of 802.11n are optional, which means network performance will be largely a function of the hardware configuration and options implemented from the standard. Some other modifications made in the standard which contribute to its wide scope are transmit beam forming (TxBF) – using an array of antennas to steer or form a directed resultant wave; space-time block coding (STBC) – broadcasting identical streams from multiple antennas to be received by multiple antennas and using signal processing to aggregate the received signals into the original stream; and spatial-division multiplexing (SDM), which allows for antennas to create parallel streams of

data occupying the same frequencies. On top of this, 802.11n devices are able to coexist and communicate with 802.11g devices.

Table 2. Summary of 802.11 physical layer standards.

Standard	Year	Modulation	Frequency [GHz]	Maximum physical layer data rate [Mb/s]
802.11	1997	FHSS	2.4	1
		DSSS	2.4	2
802.11 a	1999	OFDM	5.5	54
802.11 b	1999	DSSS	2.4	11
802.11 g	2003	DSSS	2.4	11
		OFDM	2.4	54
802.11 n	2009	OFDM	2.4	600
			5.5	600

Currently there is a purposed standard, IEEE 802.11p, that is gaining significant interest in the transportation industry. This standard, commonly called "wireless access in vehicular environment" (WAVE), operates in a licensed, but free portion of the spectrum at 5.9 GHz (Jiang and Delgrossi, 2008). This spectral range is dedicated to short range public safety-related vehicle-to-vehicle and vehicle-to-infrastructure communications and is not to be confused with the unlicensed band which is centered around 5.5 GHz. 802.11p also uses OFDM modulation, and it is expected that hardware meeting the 802.11a standard can be adapted to use this protocol. Amendments are still being proposed to the 802.11p standard, but at this time it is expected that changes will be made to the MAC layer which will increase the range and decrease the throughput compared to 802.11a (Tonguz et al., 2010).

Table 3. Relative Advantages and Disadvantages of 802.11a, b, and g (Reproduced from Behzad, 2008).

Standard	Existing Base	Data Rate	Range	Lack of Interferers	Spectrum Availability	Power Consumption	System Cost
802.11b	++++	+	++++	+	+	++++	++++
802.11a	+	++++	+++	+++	+++	++	++
802.11g	++	++++	++++	+	+	+++	+++

3.5 Radio Propagation Fundamentals

Wireless communications is accomplished by using a transmitter and receiver that emit and receive electromagnetic (EM) waves. Ideally EM waves are freely propagated without any destructive alteration and are only governed by the physics of free space propagation. In practice, many factors can alter or disrupt EM wave propagation such as reflection, diffraction, absorption, and multipath effects. While it is not always possible to eliminate these effects, it is desirable to understand their underlying principles, learn to identify their effects, and know how to minimize undesirable influence from these factors.

3.5.1 Free Space Propagation

The free space propagation model given by Rappaport (2002) shows that the received power, P_r , is a function of the transmitted power, P_t , the transmitting and receiving antenna gains, G_t and G_r , the wavelength of the EM wave, λ , and the distance separating the transmitter and receiver, d .

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2} \quad (1)$$

Equation (1) assumes no internal transmitter or receiver losses, P_r and P_t are in the same units, G_t and G_r are dimensionless quantities, and λ is related to the carrier frequency, f , by

$$\lambda = \frac{c}{f} \quad (2)$$

where c is the speed of light in a vacuum and assumed to be 299,792,458 meters / second. The energy field can also be related to the transmitted power by

$$E = \frac{P_t G_t R_{fs}}{4\pi d^2} \quad (3)$$

where P_t is the transmitted power, G_t is the dimensionless gain of the transmitting antenna, R_{fs} is the intrinsic impedance of free space which is assumed to be 377Ω , and d is the distance from the transmitter in meters.

Equation (1) shows that for a given system where P_t , G_t , G_r , and λ are constant, P_r is inversely proportional to the square of the transmission distance. Because of this relationship, it is common for the receiver power to change orders of magnitude relative to the transmit power for a given system. Hence, decibels (dB) are used to express the relationship between transmit and receive power. Expressed in decibels, path loss, PL , can be defined as the ratio of transmitted to received power.

$$PL[dB] = 10 \log \frac{P_t}{P_r} \quad (4)$$

In Equation (4), PL represents the signal attenuation as a positive quantity. Substituting Equation (1) into Equation (4) yields

$$PL[dB] = -10 \log \frac{G_t G_r \lambda^2}{(4\pi)^2 d^2} \quad (5)$$

Equation (5) can then be rearranged a number of ways to separate individual contributors to the path loss. Equation (6) is one example of this.

$$PL[dB] = -10 \log G_t - 10 \log G_r - 20 \log \frac{\lambda}{4\pi} + 20 \log d \quad (6)$$

Substituting Equation (2) into Equation (5) and further rearranging yields

$$PL[dB] = -10 \log G_t - 10 \log G_r + 20 \log f + 20 \log d - 147.552 \quad (7)$$

Equations (6) and (7) show increasing frequency and distance result in increasing path loss at a rate of 20dB/decade. Also, increasing the gain of the receiving or transmitting antennas reduces path loss.

3.5.2 Definition of dBi and dBm

Decibels are dimensionless relative values and require a defined reference in order to make them absolute. Two standards are commonly used to provide clarity when working with wireless networks. A dBi is defined as the gain relative to an ideal isotropic antenna (Reed, 2009). A dBm is a power measurement relative to 1 milliWatt fed into an object such as an antenna with a 50 ohm impedance (Reed, 2009). Antenna gains are commonly referenced in dBi, and radio transmission power levels are typically referenced in dBm. For the remainder of this work, all power levels are considered to be in units of dBm, and gains and losses are assumed to be in units of dBi.

3.5.3 Reflection

Signal reflections occur when a propagating wave bounces off a surface of which the dimensions are much larger than the wavelength. Some examples for sources of signal reflections are buildings, walls, and the earth's surface. The theory behind signal reflections is based on Maxwell's Equations and Snell's Law where a portion of the incident wave is reflected and the other portion is transmitted. Figure 6 depicts an incident wave with energy field E_i , a reflected wave with energy field E_r , a transmitted wave with energy field E_t , and a grazing angle θ_i .

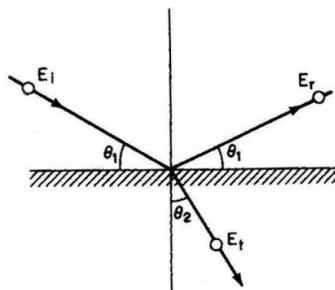


Figure 6. Diagram showing incident wave, reflected wave, transmitted wave, and grazing angle (Lee, 1997).

Equation (7) defines the reflection coefficient, RC , as the ratio of energy reflected to the energy of the incident wave

$$RC = \frac{E_r}{E_i} \quad (8)$$

where the range of the reflection coefficient is $-1 < RC < 1$ and a RC value of -1 indicates a phase difference of 180° between the incident and reflected waves.

When the propagating wave is traveling in free space, the transverse magnetic (TM) and transverse electric (TE) reflection coefficients, RC_{TM} and RC_{TE} , are calculated using

$$RC_{TM} = \frac{-\epsilon_r \sin \theta_1 + \sqrt{\epsilon_r - \cos^2 \theta_1}}{\epsilon_r \sin \theta_1 + \sqrt{\epsilon_r - \cos^2 \theta_1}} \quad (9)$$

$$RC_{TE} = \frac{\sin \theta_1 - \sqrt{\epsilon_r - \cos^2 \theta_1}}{\sin \theta_1 + \sqrt{\epsilon_r - \cos^2 \theta_1}} \quad (10)$$

where ϵ_r is the relative permittivity of the reflecting medium. Table 4 lists the relative permittivity for some common reflecting mediums.

Table 4. List of relative permittivity for common reflecting mediums (Lee, 1997).

Medium	Permittivity
Copper	1
Seawater	80
Rural ground (Ohio)	14
Urban ground	3
Fresh water	80
Turf with short, dry grass	3
Turf with short, wet grass	6
Bare, dry, sandy loam	2
Bare, sandy loam saturated with water	24

Figure 7 and Equations (8) and (9) show that for a grazing angle of zero, a flat object will become a perfect reflector, and for small grazing angles, the reflection coefficient will have a magnitude near unity.

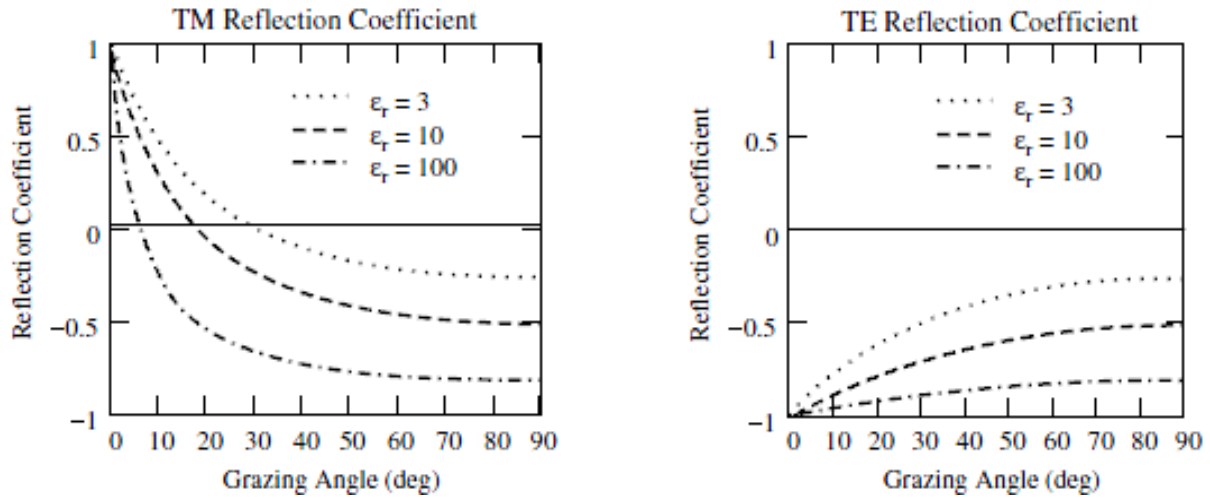


Figure 7. Reflection coefficient versus grazing angle for both magnetic and electric portions of a wave (modified from Seybold, 2005).

Rappaport (2002) showed that when reflection occurs, the resultant field at the receiver, E_{TOT} , is the addition of the direct or line of sight field, E_{LOS} , and the reflected field, E_r or E_g (Figure 8).

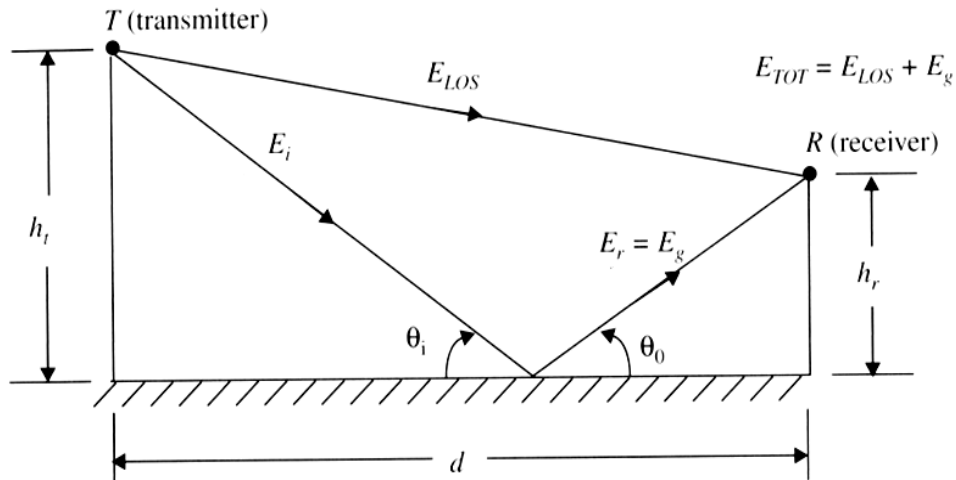


Figure 8. Diagram showing incident, reflected and direct waves (Rappaport, 2002).

$$E_{TOT} = E_{LOS} + E_G \quad (11)$$

Making the assumption that $d \gg (h_t + h_r)$ (Figure 8), Rappaport derives an equation for the total magnitude of the field at an arbitrary distance, d_0 , from the transmitter

$$|E_{TOT}| = \frac{2E_0d_0}{d} \sin\left(\frac{2\pi h_t h_r}{d\lambda}\right) \quad (12)$$

If Equation (12) is evaluated for the field strength at the receiver, $d_0 = d$, it can be shown that the magnitude of the field will be cancelled out when the following is true.

$$\frac{2\pi h_t h_r}{d\lambda} = \pi, 2\pi, 3\pi, \dots \quad (13)$$

3.5.4 Diffraction

Diffraction occurs when a wave has to travel around an object in order to propagate from transmitter to receiver. In order for diffraction to occur, the surface the wave must travel around must have dimensions that are large compared to the wavelength. In practice, diffraction is hard to accurately predict with loss predictions consisting of a theoretical approximation modified by empirical corrections (Rappaport, 2002). Models have been developed for some simple cases of diffraction, but they are beyond the scope of this work. Common sources of diffraction are buildings, hills, vegetation, and other structures.

3.5.5 Multipath

Multipath interference occurs when the transmitted signal is reflected many times and the reflected signals arrive at the receiver with varying phase shifts, causing the received wave to be distorted (Figure 9). Characteristics of multipath interference are random signal variations with respect to location and time. As with diffraction, it is challenging to determine signal attenuation levels for multipath conditions and is the current subject of advanced modeling research (Reed et al., 2009).

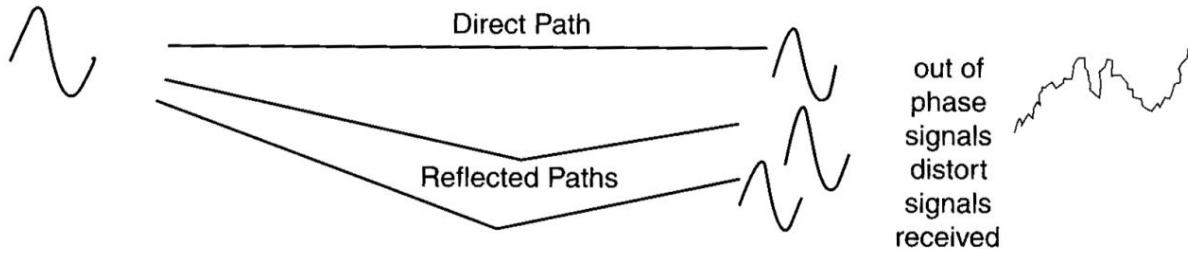


Figure 9. Illustration of multipath signals distorting the original transmitted signal (Olexa, 2005).

3.5.6 Fresnel Zones

Fresnel zones are virtual geometric regions, subdivided from the propagation space between the transmitter and receiver (Figure 10). Fresnel zones take the form of an ellipsoid with foci located at the transmitter E and receiver R and the following property holds true

$$EM + MR = ER + \frac{n\lambda}{2} \quad (14)$$

Assuming that $d \gg r_n$, the radius of the n^{th} ellipsoid, r_n , can be calculated using the following equation.

$$r_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}} \quad (15)$$

It can also be shown that when the maximum radius of the n^{th} ellipsoid is equivalent to the ground clearance of the line of sight propagation path at that point, the line of sight wave and reflected wave have lengths that are $n\lambda/2$ different (Rappaport, 2002). When n is an odd integer, the interference is constructive, and when n is an even integer, the interference is destructive (Figure 11). Additionally, it has been shown that to prevent signal attenuation due to diffraction, at least 55% of the first Fresnel zone should be kept clear (Figure 11).

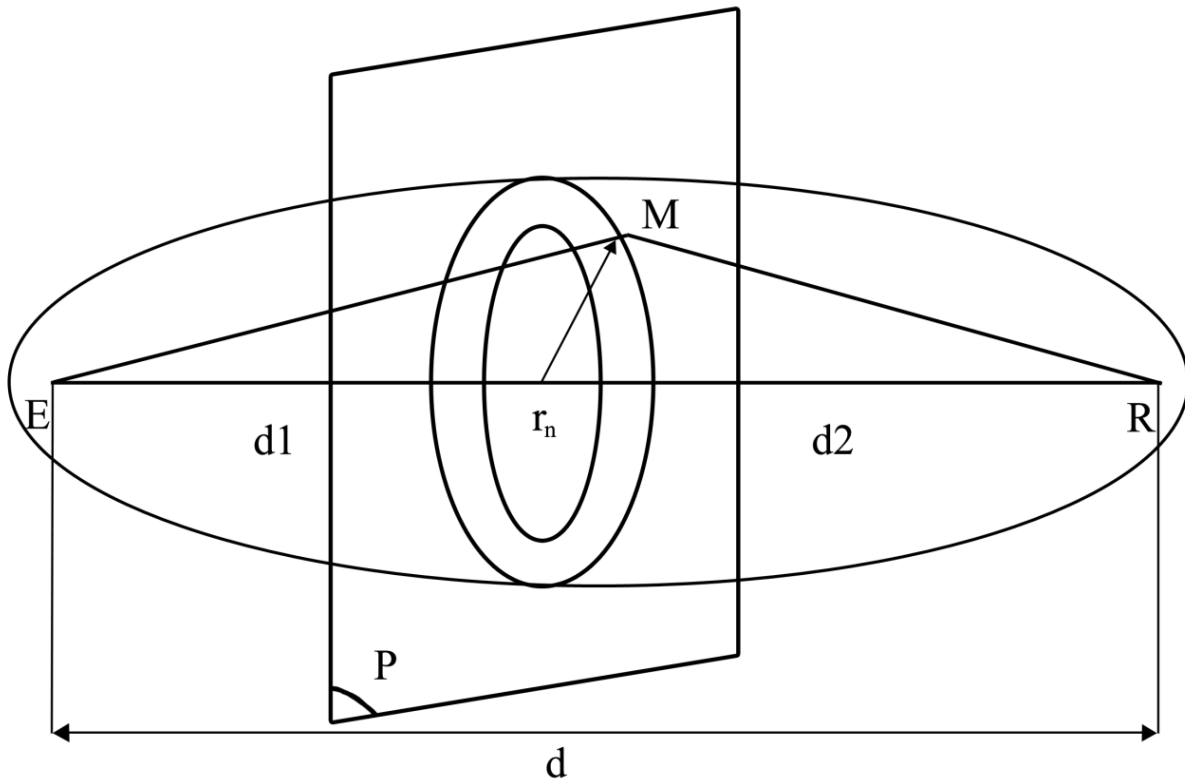


Figure 10. Schematic representation of Fresnel Ellipsoids (modified from Sizun, 2005).

Tate et al. (2008) observed that prediction of signal strength for wireless sensor networks in agricultural field environments could be improved by accounting for Fresnel zone clearance and reflections associated with proximity to Fresnel zones.

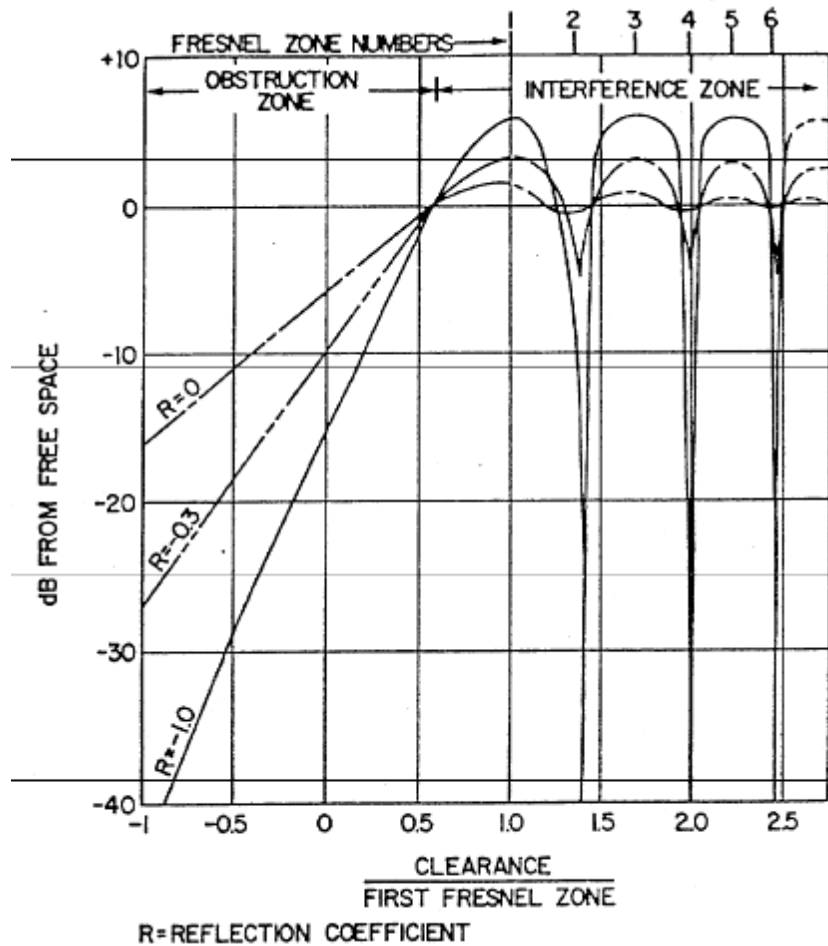


Figure 11. Diffraction and reflection signal attenuation and their relationship to Fresnel zone clearance (Lathi, 1965).

3.5.7 Link Budget Analysis

Besides the attenuation sources already listed, free space path loss is not the only source of attenuation in a wireless system. Given the logarithmic nature of free space path loss, it is important to preserve as much power as possible in a communication link. A 6dB change in signal power will double or half propagation distance. Rain, atmospheric losses, and white noise can each further attenuate a signal. Increasing the transmit power, antenna gains, and decreasing data rate to increase receiver sensitivity can all increase system performance. The Federal Communications Commission (FCC) limits the maximum Equivalent Isotropically Radiated Power (EIRP) to 36 dBm (FCC, 2009). In simple terms, this means the maximum radio frequency power that can be emitted at the transmitter's antenna is 36 dBm. Assuming no loss

in connectors or cables and a radome is not covering the antenna, the calculated EIRP (P_{EIRP}) is given by Equation (16)

$$P_{EIRP} = P_t + G_{at} \quad (16)$$

where G_{at} is the gain of the transmitter's antenna in dBi.

A typical wireless system's received power P_r can be estimated by Equation (17):

$$P_r = P_t + G_T - L_T \quad (17)$$

where P_t represents the transmitted power, G_T represents the total gains of the system, and L_T represents the total losses of the system. If the received power is less than the receiving device's sensitivity S_r , the transmission will not be successful. Link margin, LM , is defined as the difference between the received power and receiver's sensitivity.

$$LM = S_r - P_r \quad (18)$$

A high link margin indicates a more robust link than a low link margin.

A link budget is a compilation of all of the gains and losses in a communication link. While modeling and accounting for all gains and losses is not the goal of this work, portions of a link budget can be useful to help analyze various aspects of the system. Table 5 shows a sample link budget that can be used as a guide, though it should be noted that formats for link budgets vary greatly in detail and form.

Table 5. Sample Link Budget (Reproduced from Seybold, 2005).

Source	Gain	Units
Tx Power	10.0	dBm
Tx Loss	-1.5	dB
Tx Antenna Gain	32.0	dB
Radome Loss	-2.0	dB
EIRP	38.5	dBm
Path Loss (FSL)	-130.2	dB
Tx Pointing Error	-1.0	dB
Rain Loss (0.999)	-15.0	dB
Multipath	-2.0	dB
Atmospheric Loss	-0.2	dB
Total Path Losses	-148.4	dB
Radome Loss	-2.0	dB
Rx Antenna Gain	32.0	dB
Polarization	-0.2	dB
Rx Loss	-2.0	dB
Rx Pointing Error	-1.0	dB
Total Rx Gain	26.8	dBm
Interference Margin	-1.0	dB
RSL	-83.1	dBm
Rx Noise Figure	7.0	dB
Total Noise Power	-93.0	dBm
Threshold	-88.0	dBm
Net Margin	3.9	dBm
Notes		
Frequency	38.6	GHz
Wavelength	0.0078	m
Link Distance	2.0	km
Noise Bandwidth	25.0	MHz
Signal-to-Noise Ratio	8.9	dB
Polarization	Vertical	

3.6 Suitability of 802.11 in Vehicular Networks

Singh et al. (2002) conducted tests deploying an 802.11b network on automobiles. Singh et al. (2002) was able to maintain a network connection at distances of up to 1000 meters, successfully completed transmissions at speeds up to 96 kph, and showed improved connectivity through reduction of packet sizes. Bergamo et al. (2003) also ran tests using 802.11b at speeds up to 240 kph and noted no effects on performance. Bergamo et al. further noted that it took considerable time to hand off or transition between networks and the network did not perform well with the use of TCP packets, recommending the use of UDP packets. Ott and Kutscher (2004) performed tests on the Autobahn in Germany using one 802.11b transceiver on an automobile and another on a tower in a fixed location showing 150 meters usable communication radius around the tower. Ott and Kutscher (2004) also noted that TCP packets perform well when towers are topologically close, suggesting TCP might be usable when a robust connection can be obtained. Gass et al. (2006) also did similar experiments to Ott and Kutscher but made the observation that access points could detect the presence of a network much farther away than they could associate with the network, which suggests the association process could cause hysteresis in the bandwidth versus distance measurement.

Wellens et al. (2007) and Shen et al. (2009) compared the performance of 802.11a, b, and g in vehicular scenarios, both finding 802.11a performed the least satisfactory, being unstable and having the shortest range. Wellens et al. (2007) and Shen et al. (2009) also found that 802.11b and g supported communication over longer distances, with 802.11g offering the highest throughput at close range and 802.11b offering the largest range. Wellens et al. also concluded that network performance can be network dependent and stated that rate adaptation mechanisms need to be designed for changing environments in order to not impede performance. Riblett and Witzke (2009) also observed noisy degradation in performance of an 802.11g network and concluded that 802.11g is very susceptible to multipath interference, but otherwise works well in outdoor vehicular scenarios. This observation is also supported through modeling and research done by Alexander et al. (2007) and Matolak (2008) on the OFDM physical layer in the 802.11g standard. Alexander et al. (2007) and Matolak (2008) show that in outdoor environments, multipath can induce large Doppler shifts in the reflected waves, causing

interference between adjacent symbols in the OFDM subchannels which is not observed in indoor environments.

3.7 Summary

Wireless networks are complex entities that use multiple protocols and standards at different layers to connect two or more devices. 802.11 is a low level protocol defining function at the physical and data link layers of a network. Since the initial standardization in 1997, many amendments have been offered to 802.11, with the most widely used being 802.11b, 802.11g, and 802.11n. These amendments have maintained backwards compatibility for the most widely used options while updating the protocols to improve performance. A new amendment, 802.11p, is being drafted for the purpose of safety-related vehicular communication, and is of particular interest to the automotive industry.

By United States law, radios can only emit 36dBm EIRP, and in free space the power density decreases as a function of distance at 20 dBi/decade and a function of frequency at 20 dBi/decade. Other factors that influence the performance of a wireless network are reflection, diffraction, and multipath. A Fresnel zone is also an important geometric feature to a communication link, and some important behaviors of a network are related to the Fresnel zone's dimensions.

802.11 networks were designed for indoor use and do not perform optimally in an outdoor environment. 802.11a, b, and g networks have been tested in an automotive environment. 802.11a performed poorly, which is expected due to its higher frequency. 802.11b and g both operate at 2.4 GHz but use different modulation techniques, DSSS for 802.11b and OFDM for 802.11g. OFDM modulation technology was designed to reject multipath interference better than DSSS, but the specific implementation in 802.11g does not leave sufficient spacing between symbols. Thus, in practice, 802.11b performs better in outdoor environments where multipath is present.

CHAPTER 4: SYSTEM DESIGN AND VALIDATION

A simple two node network between two tractors was constructed for performance testing. Tests were devised that allowed both vehicles to be operated simultaneously in order to reduce the influence of localized conditions and provide as realistic of a test environment as possible. Personal computers (PCs) on each tractor executed an identical application that created both a server and client on each tractor with the client sending data to the opposite server over the network. Georeferenced logs were created for sent and received data on both servers and clients for post-processing. The hardware setup, radio and network configuration, software design, system validation tests, and test procedures are covered in detail in the following sections.

4.1 Hardware Setup

Figure 12 shows the hardware setup used for the in-field testing in this work. A John Deere 2955 tractor and John Deere 7700 tractor were used to mount the equipment for testing. GPS units were mounted to the cab roof using standard brackets purchased from the equipment manufacturer.



Figure 12. Two tractors fitted with GPS hardware and radios for field tests.

The GPS unit was mounted longitudinally down the center of the tractor, almost directly above the rear axle. The 802.11 radios were mounted directly to the side of the GPS unit by 50 cm and oriented so the cross-section of the radio would provide the least obstruction to GPS signals, as shown in Figure 13. The lowest point of the 802.11 radio antenna was at least 23 cm taller than the next tallest object (the GPS) in order to eliminate any interference from the GPS unit or the cab roof. Because the heights of the cab roofs were different, brackets that attached the radio to the tractor were made so the distance from the ground to the radio was the same for each unit. The distance from the ground to the bottom of the antenna was measured and recorded for each test.

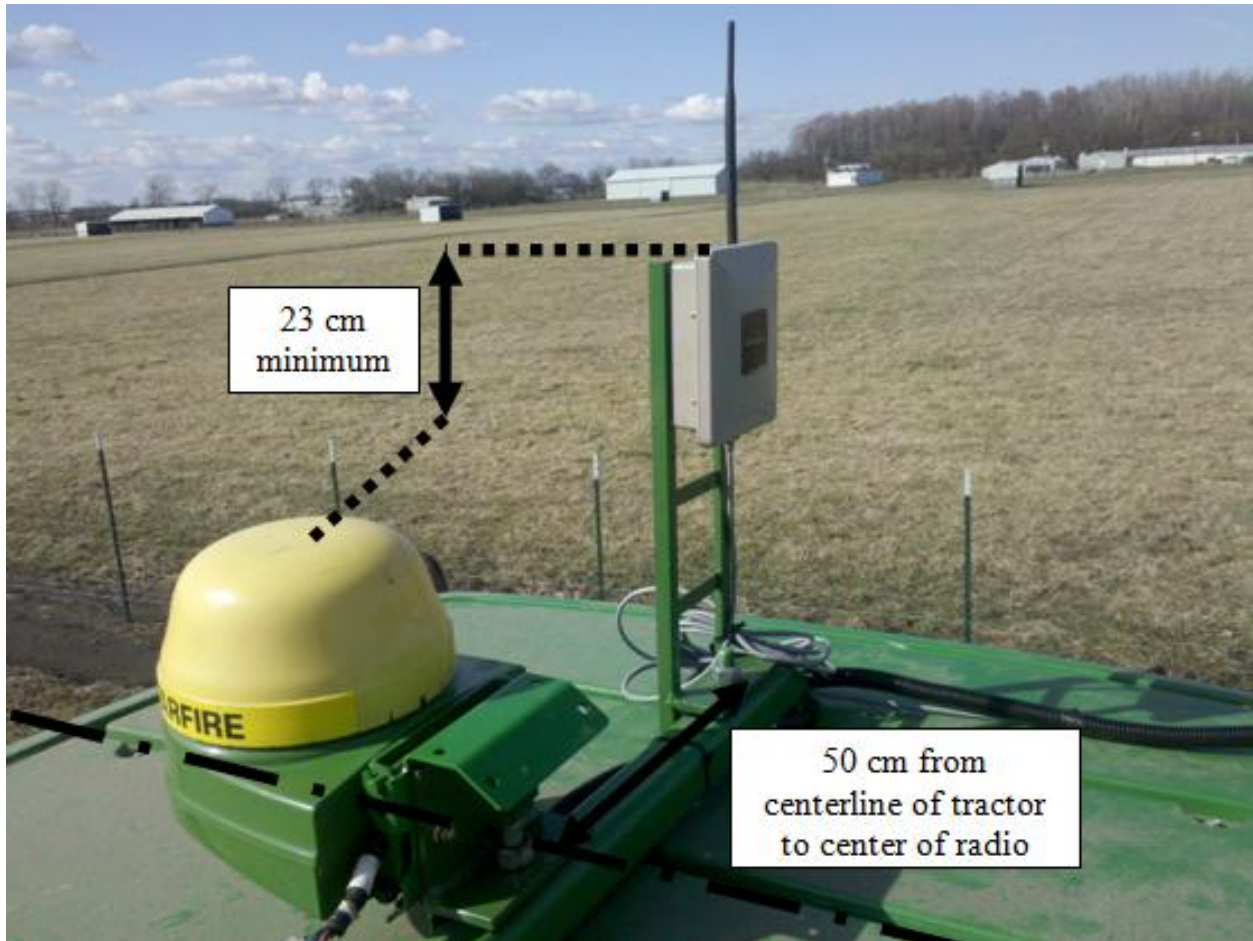


Figure 13. GPS and radio mounted on a tractor showing the layout of the units.

The GPS unit was connected electronically via OEM production wiring harnesses, part number PF90132, which extended down the corner-post into the cab. The harnessing provided RS232 NMEA output from the GPS to the laptop computer via a DB9 connector in the tractor cab as well as a CAN-bus for connection for other controllers, such as the display. The display, PN PF90423, was used to set up and configure the GPS and was also mounted in the tractor cab. The 802.11 radio had an 802.3af interface, allowing a single CAT5 cable to provide data and power to the radio. This cable was also routed down the rear corner-post of the tractor and into the cab where it was connected to an interface module. The interface module supplied power to the CAT5 cable, which ultimately powered the radio and provided a separate CAT5 cable for data interface to the laptop computer without power on the dedicated wires. A reliable power source was located to supply power both to the GPS wiring harness and the 802.11 radio.

4.2 Hardware Configuration

Figure 14 shows a system diagram for the test setup. In order for the system to function, the GPS, 802.11 radio and PC on each node must be properly configured.

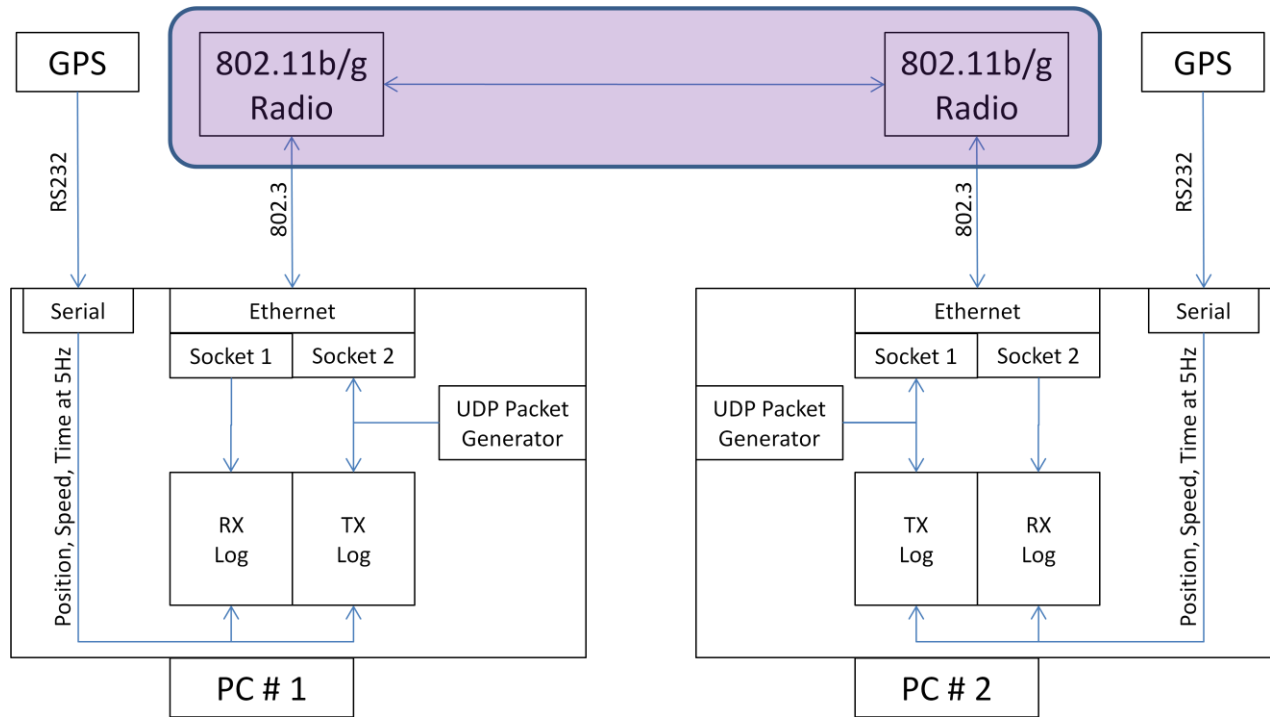


Figure 14. System architectural diagram for test setup showing 802.11 radio network and supporting hardware.

The GPS units were John Deere StarFire™ receivers using a SF1™ corrections signal with an advertised pass-to-pass accuracy of ± 25 cm (Deere and Company, 2010). The receivers were configured to output standard GGA and RMC NMEA 0183 messages at 5 Hz and 38,400 bits/sec baud.

Both laptop computers were equipped with an 802.3-2008 compliant Ethernet card as well as an RS232 port for interfacing with the test setup. The RS232 port was configured by the test software, and only the COM port number for the corresponding port was needed in advance. For the entire test duration, each computer was assigned a fixed IP address, and the Ethernet adapter had to be properly configured to use this address. The exact addresses used for each node could be changed to some extent, but an architecture with fixed IP addresses was chosen so

the network architecture could be rigidly established and consistent for all tests. Figure 15 illustrates the basic network configuration used for the laptops during testing.

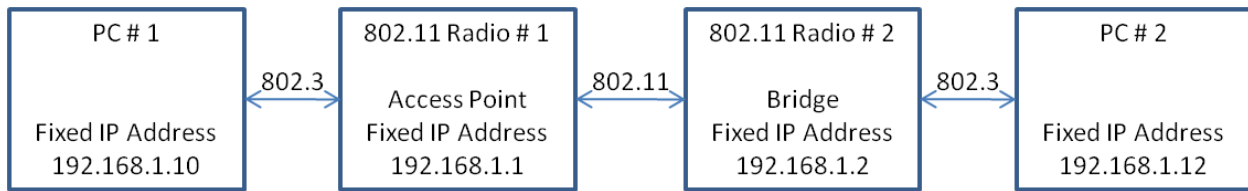


Figure 15. Network diagram of test setup.

The 802.11 radios used in this research were EnGenius™ model EOC-3220-EXT 802.11b / g compliant radios. The radios required a one-time initial configuration that is documented below as well as some changes between individual tests, which are documented later in this chapter. The process of configuring the radios was accomplished using a web browser to log into the radios. All wireless configuration instructions assumed the radios were initially configured to factory defaults. The first step was to set up one radio as a bridge and the other radio as an access point. Static IP addresses were then assigned to each radio as shown in Figure 15. After this had been finished for both radios, the radio configured as a bridge was connected to the network broadcast by the access point. Once all settings were saved, the radios could be powered down and the initial configuration was complete. Screenshots of the radio setup are included in Appendix A.

4.3 Test Software Design and Implementation

In order to measure the performance of the radio link, a software application was created to generate, send, receive, and log communications data between nodes. This application was deployed on the PCs and executed during a series of in-field tests. Significant effort would have been required for the in-field application to log data in a format that could be directly analyzed, so a second application was required to post-process the field-collected data into meaningful information that addressed the objectives of this work. Finally, Microsoft Excel™ was used to plot and statistically analyze the post-processed data. Figure 16 illustrates the flow through the collection, post-processing, and analysis processes. The in-field data collection and post-processing software is described further in this chapter, while any software related to the presentation or statistical analysis of the data is discussed in the following chapter.

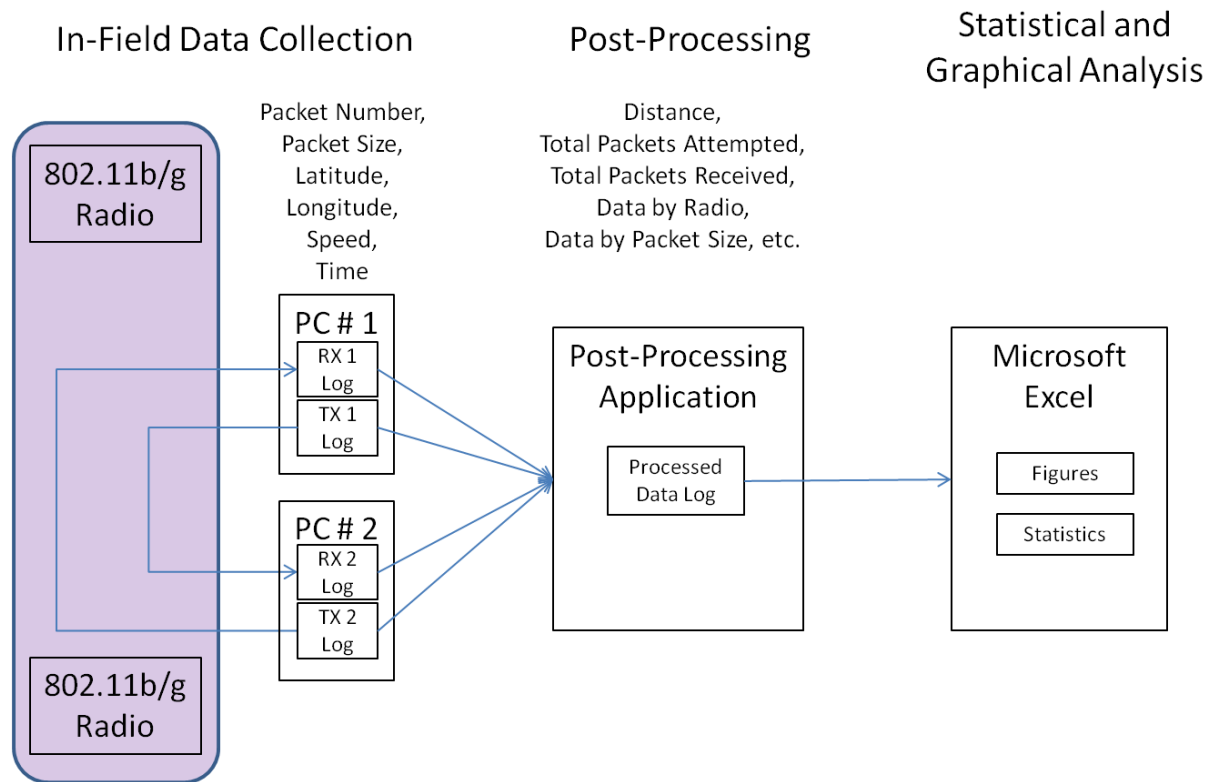


Figure 16. Flow of data through data collection, post-processing, and analysis processes.

4.3.1 In-Field Application

In order to obtain accurate and meaningful results, the in-field application was designed to fulfill a number of requirements. The application generated a packet of data to be sent over the wireless network with either a successful or failed outcome. Each packet transmission was georeferenced and logged. The application generated packets of multiple sizes in an alternating pattern and properly timed the packet transmissions so the network was never pushed beyond its specified bandwidth limits. Georeferenced logs were created for the received data. Since large amounts of data were transmitted and received over the course of a test, a file format was used that was reasonably compact and allowed for many successive tests to be conducted. The application started sending data only after it had received communication from the corresponding application at the other node in order to ensure packets were not incorrectly perceived as dropped. The tractor operator at each node had some general indication of the network connection quality so tests were not be prematurely stopped or conducted for longer times than

necessary. Finally, the application included basic diagnostics to ensure the system was functioning properly while the test is being conducted.

Figure 17 is a flow diagram of the in-field application software, and Appendix B contains the actual source code for this application. The software can be subdivided into three broad portions that correspond to each of the columns in the diagram: initialization, main loop operation, and shutdown. The application starts by prompting the user to input a series of parameters relevant to the forthcoming test. The IP address of the receiving node is required so each node knows the destination to which it needs to send its data packets. Next, the network baud rate is entered in units of Mbits/sec. This parameter is used to ensure the application does not attempt to send more data over the network than is possible. Lastly, the port number for the serial port is required so the software knows which COM port to monitor to receive GPS output. Once these three parameters are entered by the user, a series of initializations occur. These initializations are straightforward with the distinction that in all three cases, the initializations are non-blocking in nature (Microsoft, 2010). This is a way of configuring a stream so it will not block linear execution while waiting for data to be received, thus allowing the main loop to run at a rapid pace and eliminating the need for multiple threads in the application.

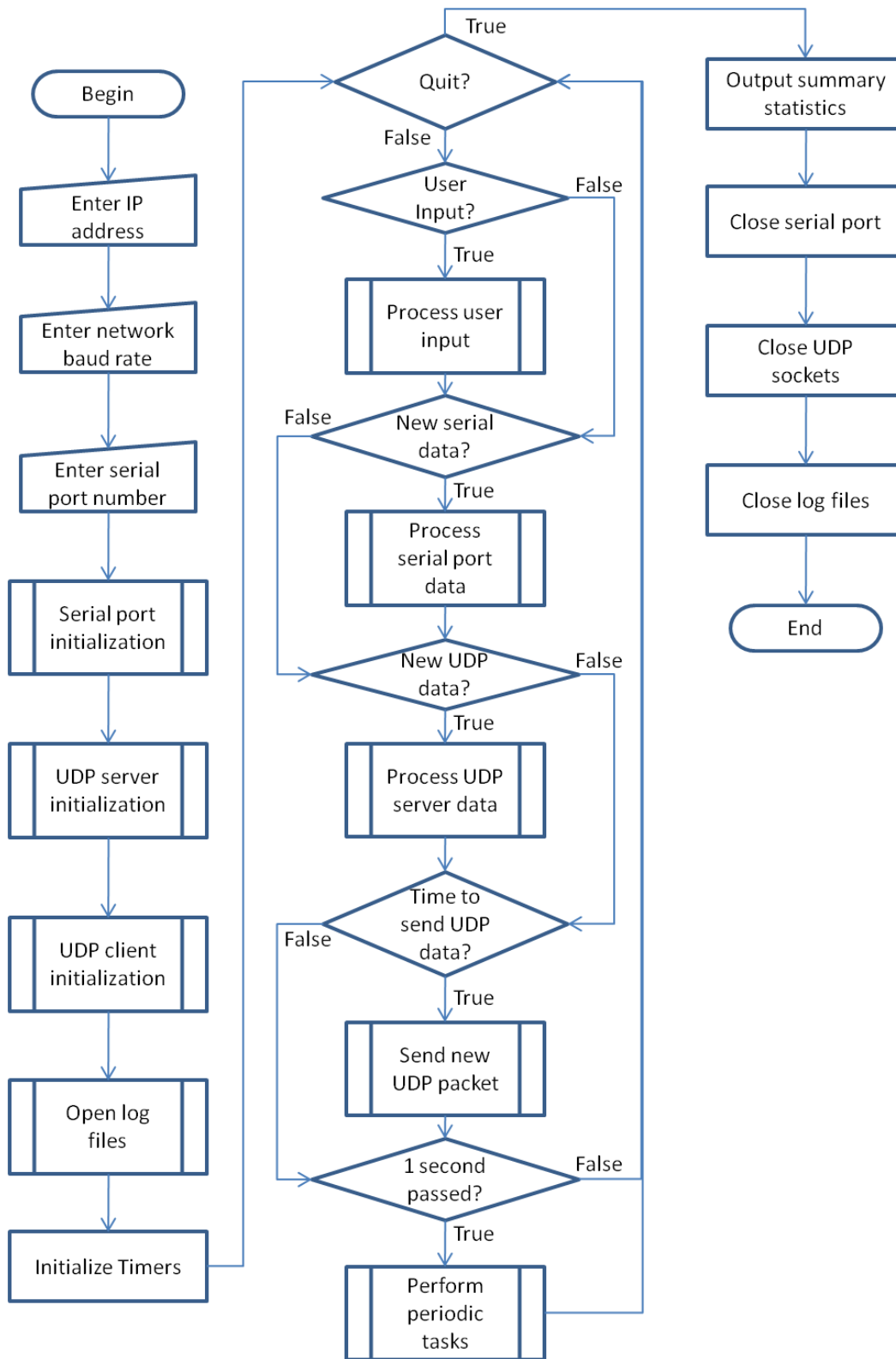


Figure 17. Flow diagram of in-field application software.

The main loop of the application is an infinite loop that cycles at a frequency greater than 1 kHz and is only terminated by typing the command "quit" into the keyboard. Each time the loop cycles, it performs five functions: handling input data, parsing GPS data, handling received data packets, sending data packets, and handling miscellaneous periodic tasks. Each of these tasks are briefly described in the following paragraphs.

The user input portion of the main loop maintains a buffer of characters entered by the user. Whenever the user presses the "enter" key, the buffer is parsed and discarded. Two commands, "start" and "quit," are supported. The "start" command initiates the transmission of a special packet over the network that, when successfully transmitted, causes both applications to start systematically sending packets of data. The "quit" command sets a flag that ultimately causes the main loop to terminate and the program to shut down.

The serial port processing portion of the main loop also maintains a serial port buffer which, upon receiving a complete NMEA type string, will parse and discard the buffer. Two types of NMEA strings, GGA and RMC, are used to determine the current velocity, position, altitude, time and date. The GPS latitude and longitude are checked for validity, and when it is determined that accurate data have been received, a flag is set. This flag is checked and reset by the periodic portion of the main loop to alert the operator if there is a problem with the GPS input.

The packet receipt and generation portion of the main loop perform the functions that are at the core of the in-field application. The tests conducted by Singh et al. (2002), Bergamo et al. (2003), Ott and Kutscher (2004) were designed to measure throughput versus distance among other factors. The objective of this work was to understand the reliability versus distance, and using TCP, which automatically retries unsuccessful packet transmissions, would unnecessarily complicate the application logic. Thus, UDP was selected as the transport layer protocol.

The maximum packet size that can be transmitted over an 802.11 physical layer is 2345 bytes (IEEE, 2007). Given that the data link, network and transport layers add 34, 12, and 16 bytes overhead, respectively, to a typical UDP packet, the maximum amount of actual data a single undivided UDP packet can transmit over an 802.11 network is 2283 bytes.

The data content of a UDP packet consists of a sequence number followed by random numbers. Figure 18 shows how the sequence number was repeated for each length packet before it is incremented. Each time a packet is queued for transfer, the theoretical transmission time, T_{TX} , is estimated using the following formula

$$T_{TX} = \frac{L * CPU * 100}{R * SF} \quad (19)$$

where L is the packet length in bytes, CPU is the CPU processor speed in cycles per second, R is the baud rate of the network, and SF is a safety factor between 1 and 100.

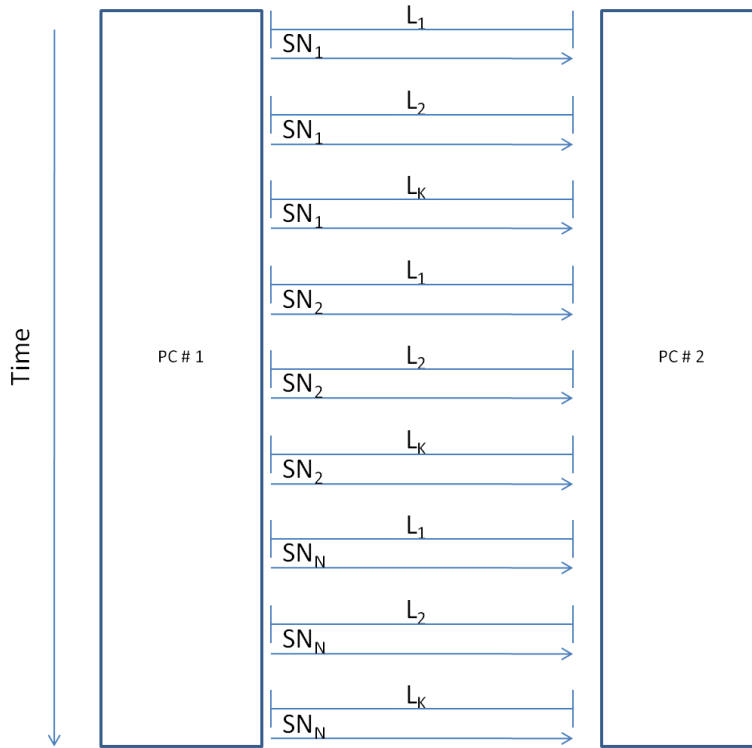


Figure 18. Illustration of sequential packet transmission with length, L , and sequence number, SN .

Each time a packet is received or transmitted, the packet sequence number, packet length, latitude, longitude, speed, and time are recorded in a comma separated value (CSV) style file. The format of all of these parameters should be self-explanatory with the exception of time,

which is expressed as the value of seconds since midnight. Separate log files were created for transmitted and received data.

The final portion of the main loop executes once every second and completes a number of low-frequency periodic functions related to the user interface display. An example of the application user interface during in-field operation is shown in Figure 19. For each packet size, the application estimates instantaneous and cumulative receipt data and displays them in a percentage format.

When the user enters the "quit" command, the main loop will terminate and the shutdown tasks will be executed. These tasks include shutting down all ports and sockets as well as outputting the total number of packets sent and received.

	Instant Receipt Statistics						Cumulative Receipt Statistics						
	L ₁	L ₂	L ₃	L ₄	L ₅	L ₆	L ₁	L ₂	L ₃	L ₄	L ₅	L ₆	
INST RX:	50	66	66	50	100	100	TOT RX:	74	73	71	67	68	56
INST RX:	100	100	100	100	100	100	TOT RX:	75	74	71	68	69	56
INST RX:	100	100	100	100	100	100	TOT RX:	75	74	71	68	69	57
INST RX:	100	100	100	100	100	100	TOT RX:	75	74	72	68	69	57
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	72	69	70	57
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	73	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	73	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	73	70	71	59
INST RX:	100	100	100	100	100	100	TOT RX:	77	75	73	70	71	59
INST RX:	16	16	16	16	16	0	TOT RX:	76	75	73	69	70	59
INST RX:	16	16	0	16	16	0	TOT RX:	76	75	72	69	70	58
INST RX:	71	71	71	71	66	100	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	100	100	100	100	TOT RX:	76	75	73	70	70	59
INST RX:	100	100	100	100	60	50	TOT RX:	76	75	73	70	70	59
INST RX:	100	100	100	100	100	100	TOT RX:	77	75	73	70	71	59
INST RX:	100	100	66	50	100	100	TOT RX:	77	75	73	70	71	59
INST RX:	33	33	50	40	16	0	TOT RX:	76	75	73	70	70	59
INST RX:	60	100	60	50	50	33	TOT RX:	76	75	73	70	70	59
INST RX:	0	14	14	0	0	0	TOT RX:	76	75	73	69	70	59
INST RX:	16	33	33	33	16	20	TOT RX:	76	75	72	69	70	58
INST RX:	100	100	66	66	33	50	TOT RX:	76	75	72	69	70	58
INST RX:	33	33	16	16	33	0	TOT RX:	76	75	72	69	70	58
INST RX:	33	33	33	16	33	16	TOT RX:	76	75	72	69	70	58
INST RX:	66	50	66	33	40	0	TOT RX:	76	75	72	69	69	58
INST RX:	50	33	50	50	33	50	TOT RX:	76	74	72	69	69	58
INST RX:	66	66	66	50	33	50	TOT RX:	75	74	72	69	69	58
INST RX:	100	100	66	66	100	66	TOT RX:	76	74	72	69	69	58
INST RX:	66	66	100	66	100	66	TOT RX:	75	74	72	68	69	58
INST RX:	66	66	66	50	33	20	TOT RX:	75	74	72	68	69	58
INST RX:	66	66	66	50	16	50	TOT RX:	75	74	72	68	69	58
INST RX:	50	50	50	50	50	0	TOT RX:	75	74	72	68	69	58
INST RX:	66	66	66	66	16	33	TOT RX:	75	74	72	68	69	57
INST RX:	33	33	33	33	20	33	TOT RX:	75	74	72	68	69	57
INST RX:	50	50	50	33	16	33	TOT RX:	75	74	72	68	68	57
INST RX:	100	100	66	66	33	50	TOT RX:	75	74	72	68	68	57
INST RX:	66	66	66	50	66	33	TOT RX:	75	74	72	68	68	57
INST RX:	50	50	50	33	33	50	TOT RX:	75	74	72	68	68	57
INST RX:	50	50	50	16	16	0	TOT RX:	75	74	71	68	68	57
INST RX:	50	50	66	66	50	20	TOT RX:	75	74	71	68	68	57
INST RX:	42	14	28	14	40	16	TOT RX:	75	74	71	68	68	57
INST RX:	50	66	16	20	16	0	TOT RX:	75	73	71	67	68	57
INST RX:	33	33	40	0	16	16	TOT RX:	74	73	71	67	67	56
INST RX:	100	40	50	50	16	0	TOT RX:	74	73	71	67	67	56
INST RX:	66	16	33	16	16	0	TOT RX:	74	73	71	67	67	56

Figure 19. Picture of in-field application user interface displaying instantaneous and cumulative number of packets received for each packet length.

4.3.2 *Post-Processing Application*

The post-processing application works in two phases as shown in Figures 20 and 21; the first phase completes the geospatial portion of the calculations, and the second phase computes and aggregates the statistical data for each packet. Data from the first phase are needed in order to complete the second phase. Figure 20 shows the processing logic in a traditional linear programming flowchart, while Figure 21 illustrates the flow of data through the post-processing application. The software initialization, two processing phases and shutdown are described in the following paragraphs.

The filenames of the four transmit and receive files serve as input to the post-processing application and are included in the command string to invoke the post-processing application. The filenames of the input files are used to generate filenames for output files and two output files are opened: one to contain the spatial information such as position, direction, etc., and the second to contain all of the distance-based statistical information.

The first processing phase seeks to compute all spatial data related to the given run. GPS data was recorded at 5Hz, but packets are sent across the network at a much higher frequency. By scanning both sets of transmit logs for unique and matching time and position-related values and only doing computations on those values, the post-processing application will eliminate many duplicate calculations in processing the packet statistics. The distance between nodes was calculated using a proprietary coordinate transformation where latitude and longitude were converted to a rectangular coordinate system and distance calculations could be done using simple algebra. A determination of whether the nodes were moving towards or away from each other was made by looking at successive distance calculations. If the distance between nodes was increasing over time, the machines are moving apart and if the distance is decreasing, the machines are moving toward each other. The output of the first processing phase is a two-dimensional array that is stored in RAM that contains time, distance, and direction for each GPS position and a spatial log file that can be used to plot out spatial information. The parameters contained in the spatial log file are described in Table 6. The file can easily be converted to a standard spatial file type using readily available programs, for example a "kml" file (Google, 2010), which is compatible with free viewers like Google Earth™.

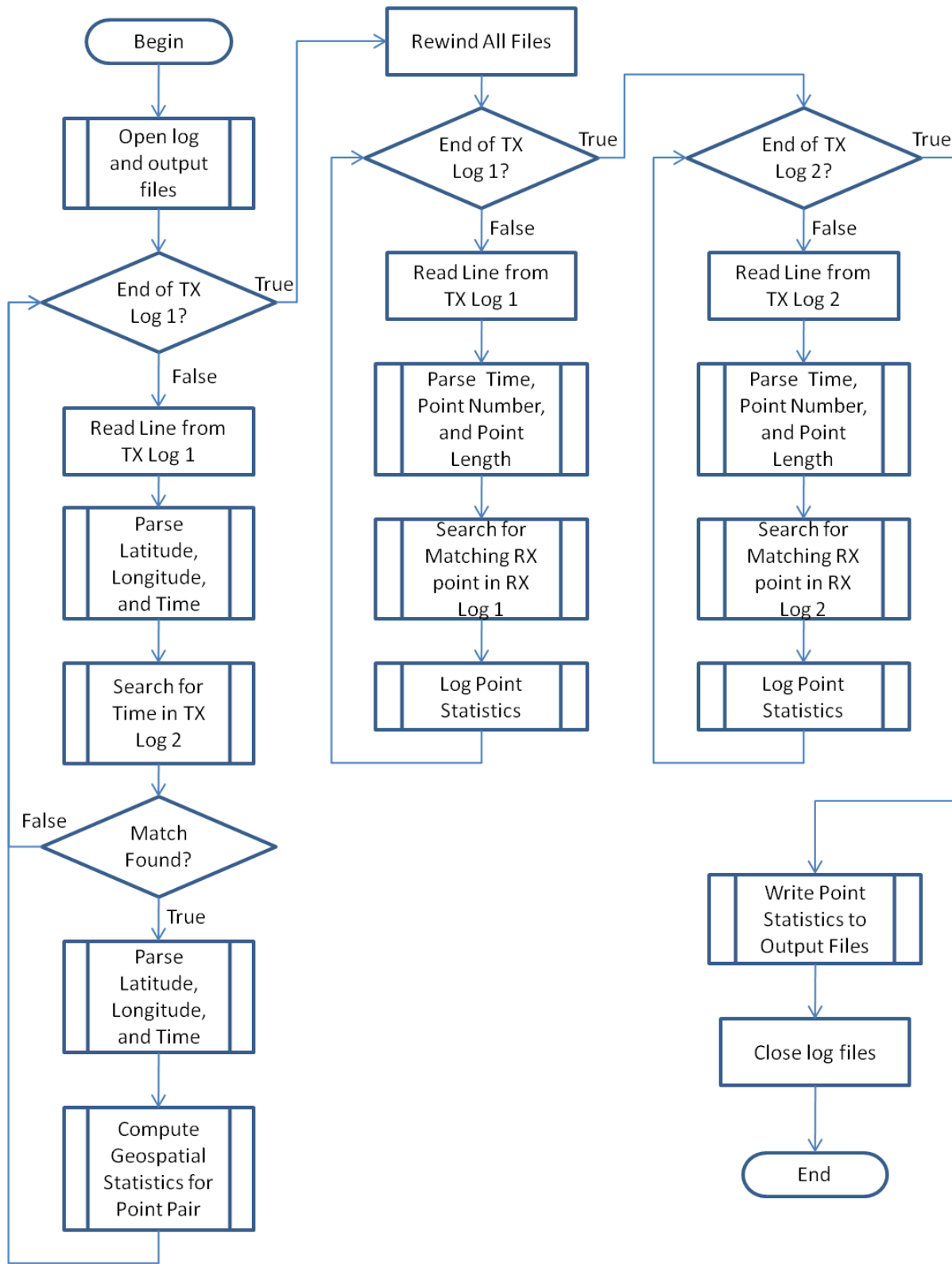


Figure 20. Flowchart of post-processing application.

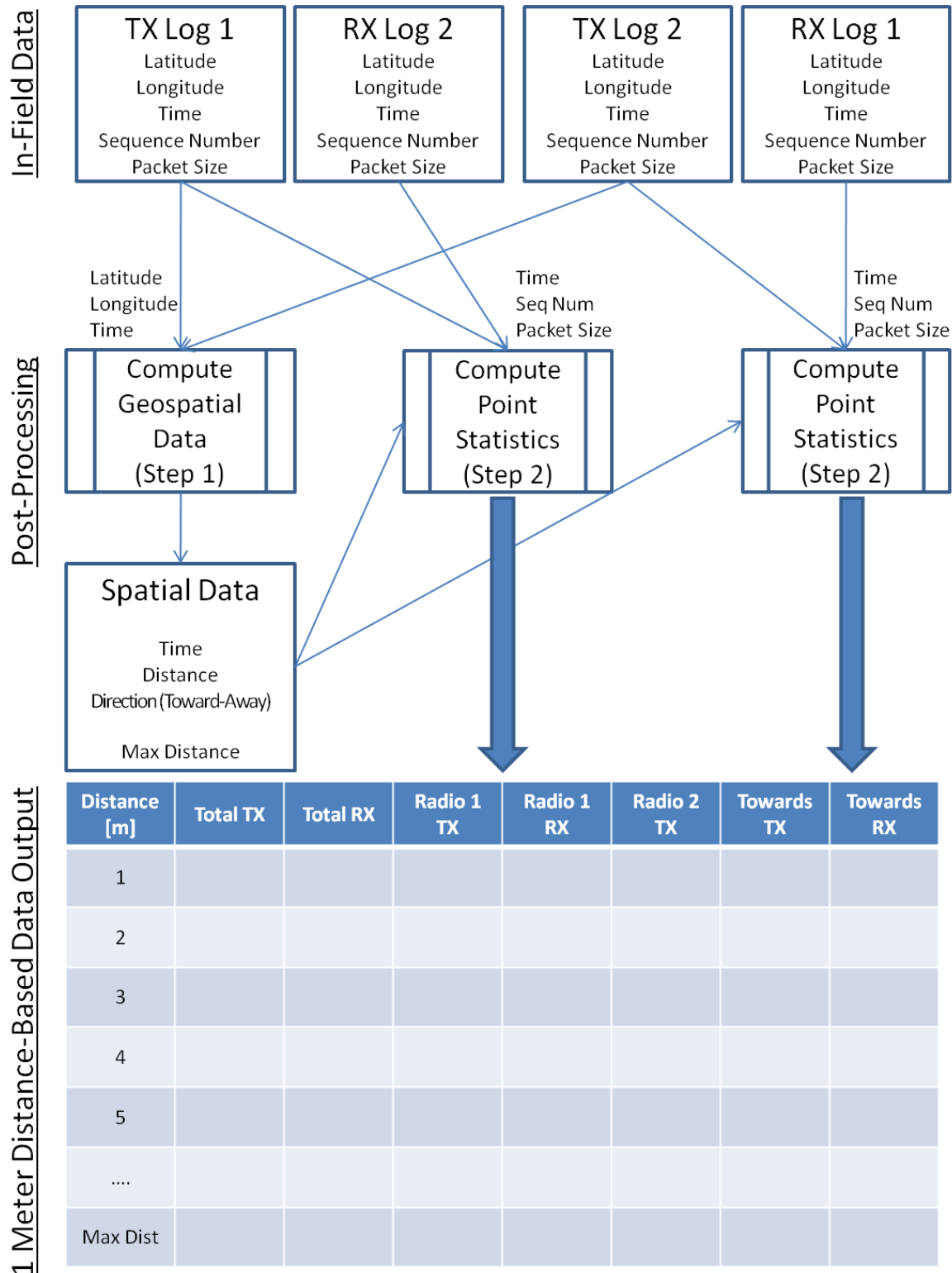


Figure 21. Illustration of post-processing application function.

Table 6. List of parameters and their descriptions in spatial output file.

Abbreviation	Description
SECS	Seconds since 12:00 AM (midnight) in units of seconds X 10
DIST	Distance between radios [m]
TOWARD	0 = Radios moving towards each other 1 = Radios moving away from each other
LAT1	Latitude of Radio 1 [decimal degrees]
LON1	Longitude of Radio 1 [decimal degrees]
LAT2	Latitude of Radio 2 [decimal degrees]
LON2	Longitude of Radio 2 [decimal degrees]

The second processing phase attempts to determine the outcome of a packet transmission by comparing the contents of the transmit and receive files. Packets from the transmit log file are examined one by one. The contents of the receive file are buffered into RAM for faster searching and processing. The time field of the transmit packet is parsed and used to quickly skip to the correct location in the receive data buffer, making the assumption that the packet will be received at the same or later time as compared with the transmitted packet. Packets in the receive log are sequentially searched until either a matching sequence number and packet length field are found, indicating a successful transmission, or the sequence number in the receive log is greater than the sequence number of the transmitted packet, indicating a failed transmission. Once the outcome of a transmitted packet is determined, all properties for that packet are known. A separate function examines these properties and maintains an aggregate statistical log in RAM. The parameters recorded in this log are listed in Table 7.

Table 7. List of parameters and their descriptions in the statistical output file.

Abbreviation	Description
D	Distance between Radios [m]
TA	Total Number of Packet Transmission Attempts for Radios 1 and 2
SA	Total Number of Successful Packet Transmissions for Radios 1 and 2
R1TA	Total Number of Packet Transmission Attempts for Radio 1
R1SA	Total Number of Successful Packet Transmissions for Radio 1
R2TA	Total Number of Packet Transmission Attempts for Radio 2
R2SA	Total Number of Successful Packet Transmissions for Radio 2
R1IBTA	Total Number of Packet Transmission Attempts for Radio 1 when machines were moving towards each other
R1IBSA	Total Number of Successful Packet Transmissions for Radio 1 when machines were moving towards each other
R2IBTA	Total Number of Packet Transmission Attempts for Radio 2 when machines were moving towards each other
R2IBSA	Total Number of Successful Packet Transmissions for Radio 2 when machines were moving towards each other
PK1TA	Total Number of Packet Size 1 (15 bytes) Transmission Attempts
PK1SA	Total Number of Packet Size 1 (15 bytes) Successful Transmissions
PK2TA	Total Number of Packet Size 2 (150 bytes) Transmission Attempts
PK2SA	Total Number of Packet Size 2 (150 bytes) Successful Transmissions
PK3TA	Total Number of Packet Size 3 (500 bytes) Transmission Attempts
PK3SA	Total Number of Packet Size 3 (500 bytes) Successful Transmissions
PK4TA	Total Number of Packet Size 4 (1000 bytes) Transmission Attempts
PK4SA	Total Number of Packet Size 4 (1000 bytes) Successful Transmissions
PK5TA	Total Number of Packet Size 5 (1400 bytes) Transmission Attempts
PK5SA	Total Number of Packet Size 5 (1400 bytes) Successful Transmissions
PK6TA	Total Number of Packet Size 6 (2200 bytes) Transmission Attempts
PK6SA	Total Number of Packet Size 6 (2200 bytes) Successful Transmissions

4.3.3 Test Software Validation

The functionality of the in-field application was validated using two test scenarios. During the first test scenario, the 802.11 radios were replaced with a crossover CAT5 cable, effectively eliminating the wireless portion of the system. Data collection was collected for 5 minutes, and the number of transmitted and received packets and bytes were compared at each node to confirm that all traffic was being accurately accounted for. A second test, which is referenced as run 19 in Table 8, was executed with the identical test setup used in the formal

experiments but with stationary tractors approximately 7 meters apart. The radios were configured to operate at 18 Mbps/sec and data collection was initiated for 161 seconds with 33,864 packets being transmitted and 33,808 packets being received, resulting in a 99.8% success rate.

4.4 Test Procedures

The University of Illinois Agricultural Engineering Farm was chosen as the site to conduct all tests for this work. This site was relatively level and free of obstructions such as trees and buildings. A site survey was conducted for competing 802.11b and g networks, and other networks were found to be present. 802.11b and g channels were selected so that there was maximum spacing between adjacent network channels to minimize interference. Data were collected in a series of 18 runs or tests over the course of two days. A summary of these runs can be found in Table 8. The data rate, protocol, and antenna height were varied as described in Table 8, with unique alterations to each test described in the "notes" column.

Table 8. Summary of runs displaying the various configurations tested.

Date	Run	Data Rate [Mb/sec]	Protocol	Antenna Base Height [m]	Antenna Tip Height [m]	Path	Notes
3/18/2010	1	1.0	b	3.38	3.63	A	
3/18/2010	2	2.0	b	3.38	3.63	A	
3/18/2010	3	6.0	g	3.38	3.63	A	
3/18/2010	4	12.0	g	3.38	3.63	A	
3/18/2010	5	18.0	g	3.38	3.63	A	
3/18/2010	6	36.0	g	3.38	3.63	A	
3/18/2010	7	54.0	g	3.38	3.63	A	
3/31/2010	8	5.5	b	3.38	3.63	A	
3/31/2010	9	5.5	b	3.38	3.63	A	1
3/31/2010	10	5.5	b	3.38	3.63	A	2
3/31/2010	11	6.0	g	3.38	3.63	A	2
3/31/2010	12	6.0	g	3.38	3.63	A	1
3/31/2010	13	18.0	g	3.91	4.16	A	
3/31/2010	14	18.0	g	3.91	4.16	A	1
3/31/2010	15	6.0	g	3.91	4.16	A	1
3/18/2010	16	18.0	g	3.38	3.63	B	
3/18/2010	17	18.0	g	3.38	3.63	A	3
3/18/2010	18	18.0	g	3.38	3.63	A	4
3/16/2010	19	18.0	g	3.38	3.63	N/A	5
Note	Explanation						
1	Instead of completing a lightbulb turn at the maximum distance between nodes, the tractors were shifted into reverse and backed along the same path to their starting point.						
2	Tractors executed a lightbulb turn while both radios were successfully completing transmissions.						
3	One tractor executed pattern A while the other tractor remained stationary.						
4	Configurations were reversed in the radios						
5	Both tractors remained stationary. Log files not created. Summary data recorded from application output.						

A typical test is illustrated in Figure 22. The test started out with both tractors within 5 to 10 meters of each other, as shown by point A. Both operators initiated the in-field application on each PC and entered the relevant information for the run. One operator entered the "start"

command to the application, and both nodes started sending packets of data. Once operators observed the application starting to output summary data similar to Figure 19, the tractors were driven forward at approximately 5 km/h at approximate right angles to each other. When both tractors reached a point, labeled point B in Figure 22, they were required to turn because of spatial constraints of the area. The tractors were always driven on grassy paths that can best be described as dividers between small plots. The most extreme points that any run reached are labeled point C in Figure 22. The distance between the nodes at these extreme points was 650 meters. If these points were at the corners of a rectangular field, the area covered would be approximately 20 hectares. Unless otherwise noted, the tractors were driven until no successful transmissions had been completed for the last 20 seconds. Then the tractors executed a lightbulb or three-point-style turn and returned to their starting location.

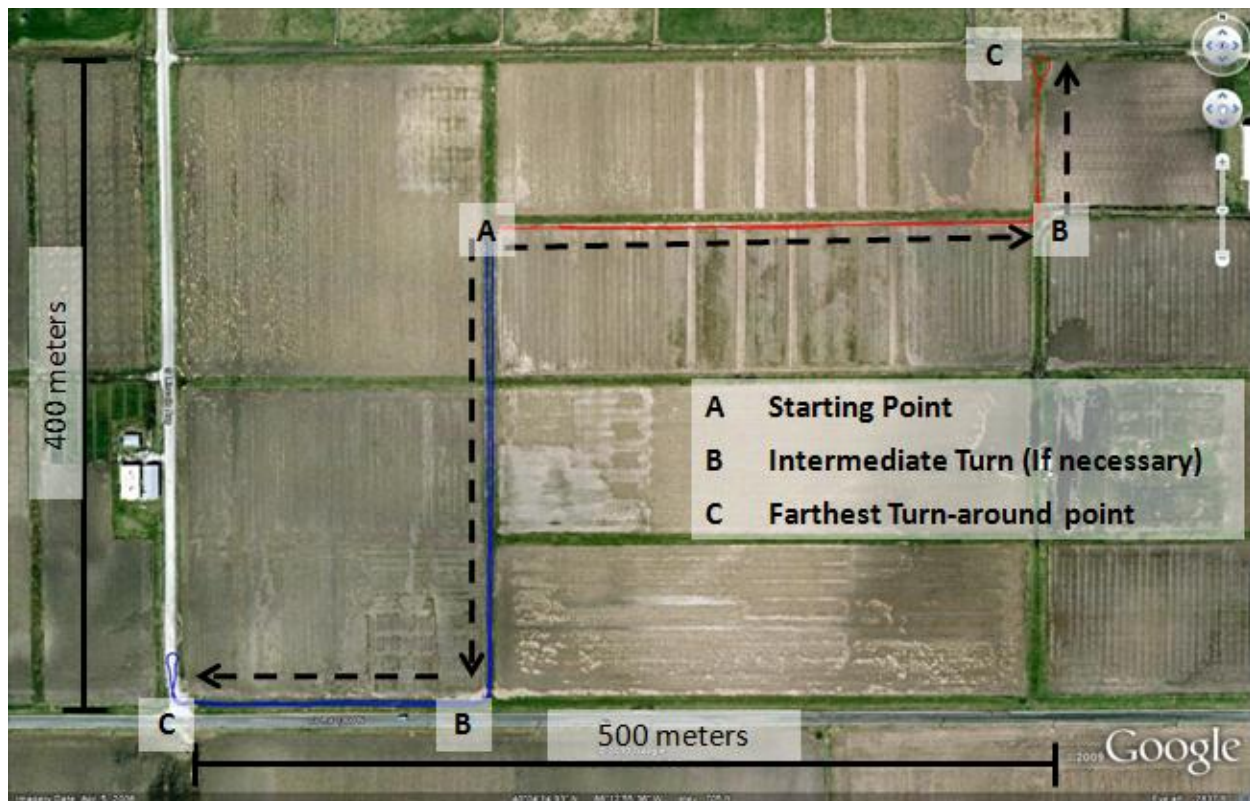


Figure 22. Normal path driven by two tractors during a data collection run.

4.5 Summary

In summary, hardware was setup on two tractors to represent a realistic in-field operational scenario to test the performance of an 802.11 network. Specifics of the hardware mounting and configuration were documented in detail. Two applications were developed to collect and post-process the data. The functionality of these applications was validated before deploying the system. A standardized test procedure was created, and various configurations of the 802.11 network were evaluated during two separate days.

CHAPTER 5: RESULTS AND DISCUSSION

An initial data set consisting of 10 runs was completed, and the analyzed data revealed some unexpected results. Distinct areas of complete packet loss and a difference in network performance based on vehicle orientation were observed. These results were investigated, and additional tests were created and executed on the second day to better understand the causes. The findings related to these two observations are discussed in the first two sections on ground reflection effects and performance differences due to orientation. The final three sections discuss the results relevant to the stated objectives of this work – namely the effects of protocol, packet size, and data rate on the performance of an 802.11 network.

The reliability versus distance of any of the 802.11 network configurations evaluated produced results that, even when averaged over one meter segments, still displayed considerable instantaneous variation. Riblett and Witzke (2009) also made this observation when trying to compare the throughput versus time, and relied heavily on data filtering and outlier elimination to process the data so descriptive statistics could be used. Some trends were more apparent than others, but in all cases, attempts were made to develop statistical approaches that mathematically quantify performance differences and have a sound theoretical and practical basis.

5.1 Ground Reflection Effects

Figure 23 represents a characteristic plot of the ratio of packets received to transmitted (expressed as a percent) versus distance. At small distances between nodes, the network performed reliably, but as distance increased, sharp unexplained drops in the network reliability were observed. These drops consistently occurred at specific distances, with smaller and more instantaneous drops at approximately 50 and 65 meters, and much more pronounced outages centered at 95 and, if applicable, 190 meters. An observational run was conducted in a different location to determine if the cause of these distinct low-performance regions was associated with a particular spatial location or if it was related to the distance between nodes. Longer duration outages were easily observed that were consistent with previous runs during this observational run by monitoring the output of the in-field application.

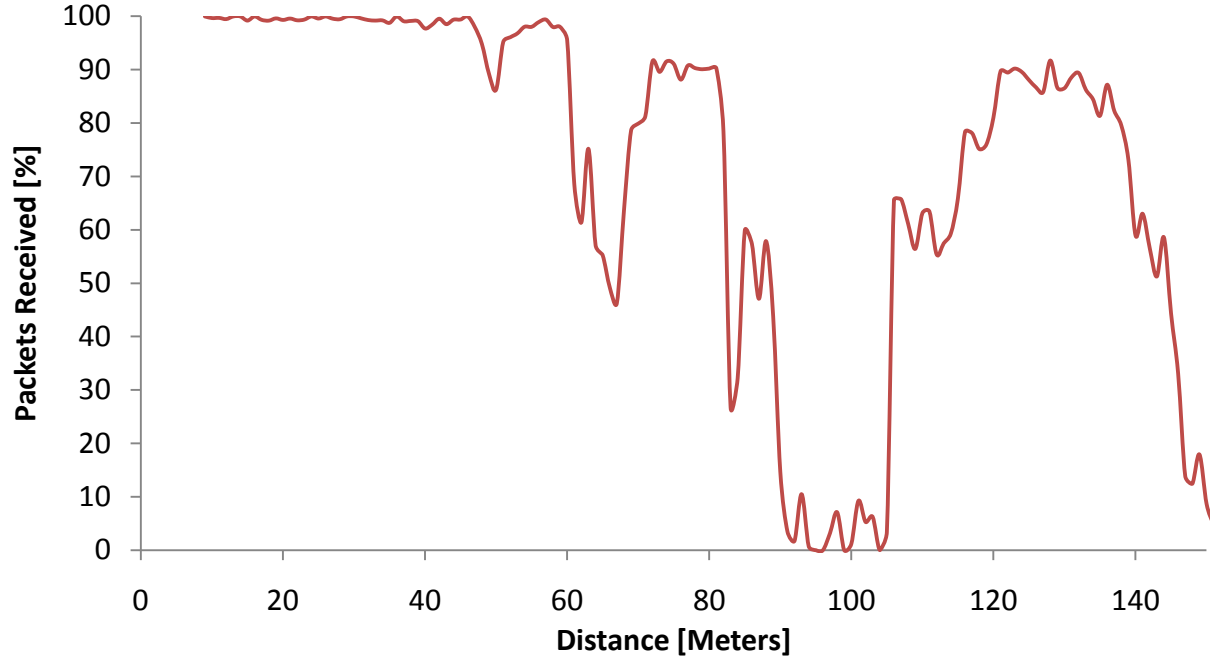


Figure 23. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 5).

Further analysis during post-processing of the first 10 runs revealed that the distances at which these drops occurred corresponded to distances between nodes where the radii of even-numbered Fresnel radius equaled the antenna heights. This observation was made by starting with Equation (15) and Figure 10 and making the assumptions that $d = d_1 + d_2$ and $d_1 = d_2$. These assumptions could be made because the antenna heights for both nodes were equal with the height measurement being made on level terrain. Using the aforementioned assumptions, Equation (15) can be rearranged to the form

$$d = \frac{4r_n^2}{n\lambda} \quad (20)$$

where $\lambda = 0.1228$ meters, r_n corresponds to the radius of the n^{th} ellipsoid and will be the same as the height of the antennas at each node, and n is the number of the Fresnel radius. Table 9 evaluates Equation (20) for antenna heights of 3.47 meters and 4.00 meters and Fresnel radii 1 through 10. It should be noted that for antenna heights of 3.47 meters, the distances between the nodes where the Fresnel radius would equal the antenna height are 65, 98, and 196 meters for

Fresnel Radii 6, 4, and 2, respectively, which correspond very well with the low-performance regions in Figure 23.

Table 9. Distance between nodes where Fresnel radius equals antenna height for the first 10 Fresnel radii.

Radius number	Antenna Height [m]	
	3.47	4.00
1	392.32	521.32
2	196.16	260.66
3	130.77	173.77
4	98.08	130.33
5	78.46	104.26
6	65.39	86.89
7	56.05	74.47
8	49.04	65.17
9	43.59	57.92
10	39.23	52.13

The distance where the even-numbered Fresnel radii equal the antenna height also corresponds to the location where the reflected wave is 180 degrees out of phase with the direct wave. The effect on the field strength at the receiving node can be calculated by rearranging Equation (12) and evaluating it at $d_0 = d$ and $h_t = h_r = h$ yielding Equation (21).

$$\left| \frac{E_{TOT}}{E_0} \right| = 2 \sin \left(\frac{2\pi h^2}{d\lambda} \right) \quad (21)$$

Evaluating Equation (21) as a function of d will yield a value ranging from 0 to 2, with a value of 0 indicating complete signal attenuation and a value of 2 indicating complete constructive amplification. Figure 24 uses Equation (21) to show that locations of complete signal attenuation also correspond to the results for even-numbered Fresnel radii in Table 9.

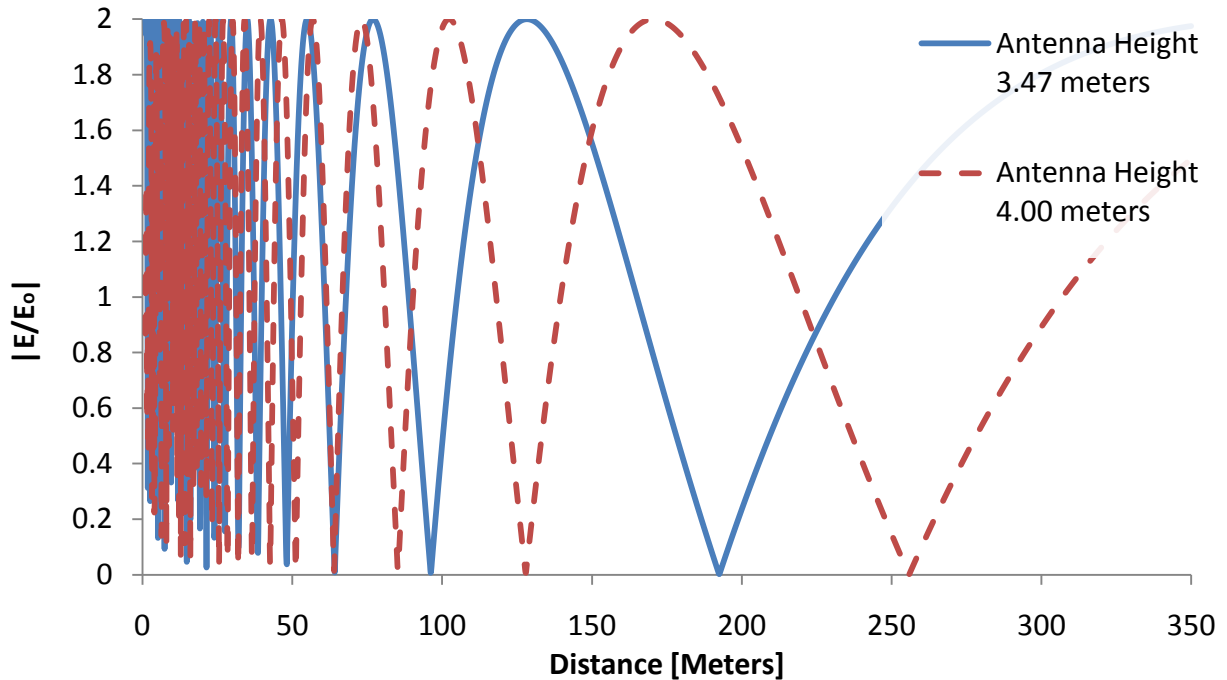


Figure 24. Plot of signal attenuation/amplification versus distance for antenna heights of 3.47 m and 4.00 m.

To further confirm this effect, the antenna height was increased to 4.00 meters for 3 runs with an expectation that a shift could be anticipated in the distances that exhibit poor performance. Figure 25 shows the performance versus distance that was typical for all 3 runs. The network in Figure 25 is identically configured compared to the network in Figure 23, with the exception that its mounting height was increased to 4.00 meters. The low-performance region is shifted near the predicted distance of 130 meters.

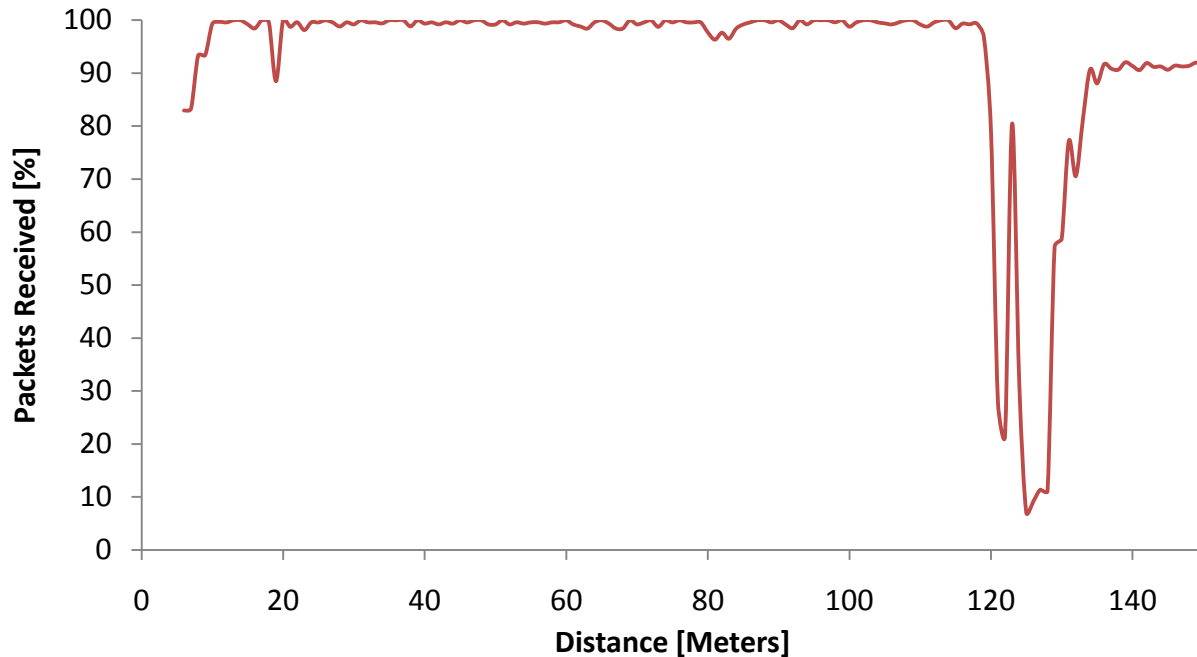


Figure 25. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 13).

Four additional observations can be made concerning signal reflections. The first is that when the distance between nodes equals the distance where the odd-numbered Fresnel radii correspond to the antenna heights, constructive signal amplification can occur. This property could potentially be utilized by more intelligent radios with multiple antennas to have a net benefit for network performance. Secondly, the small changes in topography will have large effects on the dimension of the Fresnel radii. In this work, a 0.5 meter change in antenna height caused 30-meter and 64-meter changes in distances where destructive interference occurred corresponding to the fourth and second Fresnel radii. Third, it should also be noted the field surface could be described as flat but not necessarily smooth. The field surface was fallow bean stubble and had not been leveled for irrigation or drainage purposes. Networks deployed on ground that is leveled for drainage or flood irrigation purposes could experience more pronounced reflective effects due to a more ideal reflecting surface. Lastly, it should be noted that the effect of signal reflections was never described in any previous works reviewed in preparation for this research. One possible explanation for this is that the majority of the research was performed using automobiles and the radios were mounted much closer to the ground. Decreasing the antenna height would decrease the distances where destructive signal

reflections occur. If the reflections are not perfect, only partial attenuation will occur, and if the nodes are close, the strength of the field will be high at the receiving node. This could result in a situation where reflection occurs but the attenuation is not strong enough to reduce the signal strength below the receiving node's sensitivity.

5.2 Performance Differences Due to Orientation

Figure 26 illustrates the difference in reliability for nodes that are "inbound" or moving closer together compared to nodes that are "outbound" or moving farther away from each other. This phenomenon was also consistently observed for all runs where path A was used. An observational test was completed to determine if the behavior was spatially related with the results showing that the performance differences due to orientation did not change when the location of the run was changed.

Special care was taken during the installation process to mount the radio well above any other object on the vehicle in order to reduce vehicular effects on the 802.11 network's electromagnetic waves. The radio height was increased from 3.47 meters to 4.00 meters to provide a minimum of 75 cm of clearance between the base of the antenna and next highest object on the cab roof. Figure 27 shows the results to an identical run as shown in Figure 26 with a radio height of 4.00 meters. The network with increased mounting height also performed differently based on vehicle orientation.

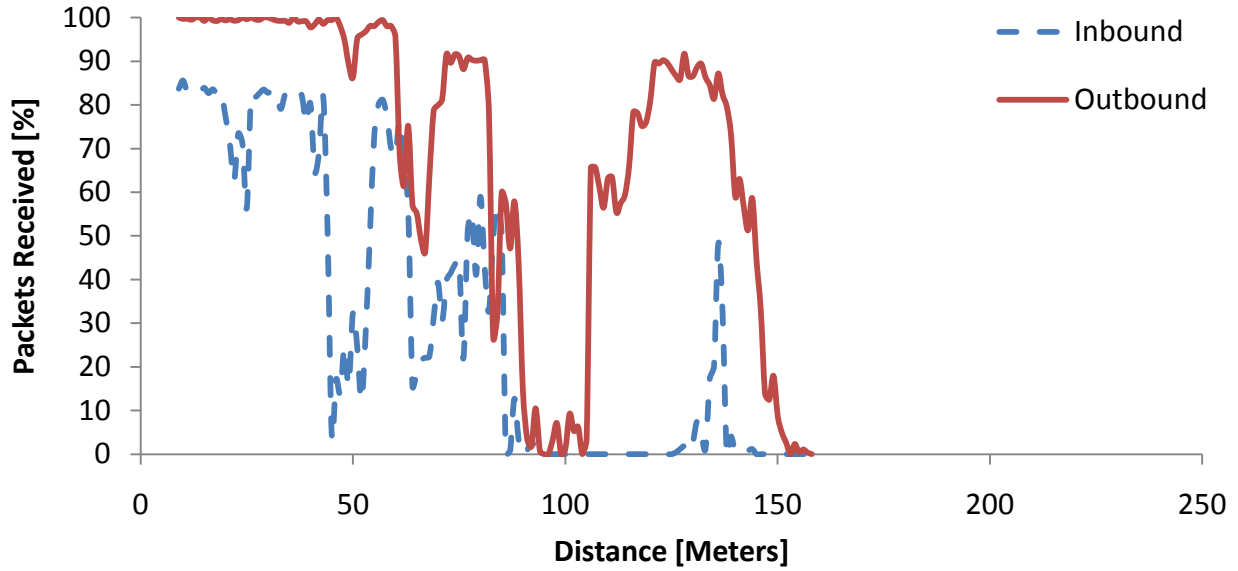


Figure 26. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters illustrating the performance difference between nodes moving closer (Inbound) to each other versus farther away (Outbound).

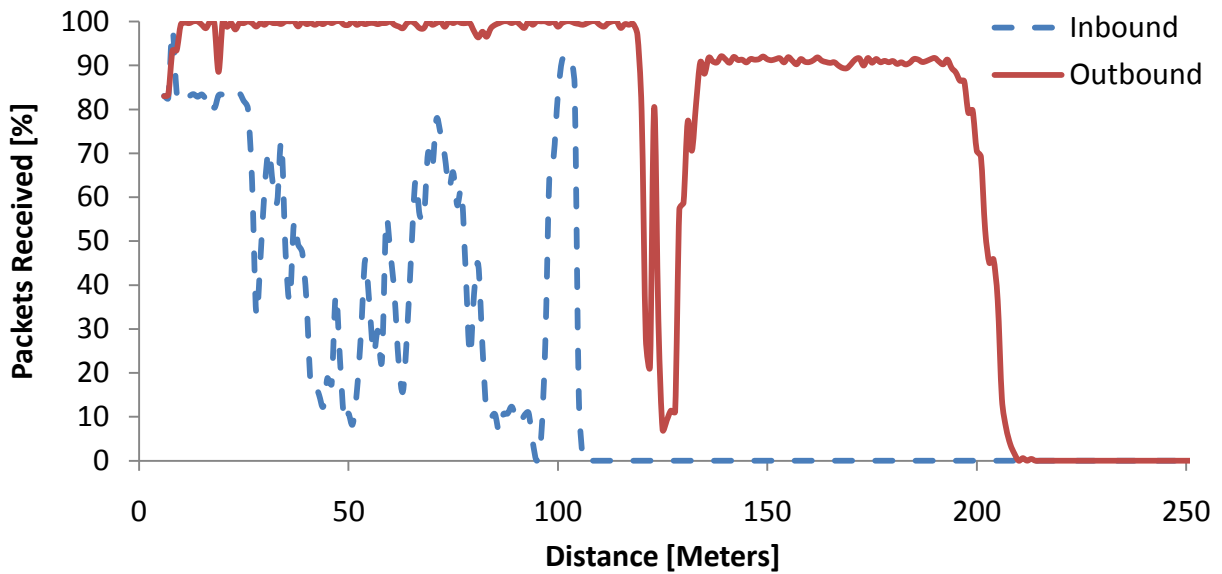


Figure 27. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters illustrating the performance difference between nodes moving closer (Inbound) to each other versus farther away (Outbound).

Another possible explanation for the difference between inbound and outbound performance is due to the overhead required to connect nodes that are currently on the same

network. Since the test procedure involved initiating the test with the nodes in close proximity and establishing a network connection, the outbound portion of a run did not have to go through an association process. However, the vehicles were operated until the connection was lost for many seconds before turning the vehicles back towards each other. Gass et al. (2006) observed that nodes could identify the presence of a network at larger distances than they could create a connection. Gass et al. also noticed a hysteresis effect, noting that a mobile vehicle passing a fixed node transmitted less data approaching the fixed node than when moving away due to the association overhead. Two alterations to the standard run were made to determine if the association overhead was producing these performance differences. The first modification was to execute a run where the tractors would turn towards each other and return to their starting points well before the network connection was lost. These runs are denoted with a "2" in the notes section of Table 8. The results from these tests still showed the same inconsistency between the inbound and outbound network performance as the original runs. It was also observed that during the turning process the connections were abruptly lost. A second modified run was performed where the vehicles were operated until they were well out of range, and instead of executing a turn and driving forward towards each other, they were driven backwards in reverse to their original position. Thus, the nodes still had to re-associate, and the nodes were moving towards each other, but the orientation of the vehicles had not changed from the outbound portion of the run. Runs that were completed using this procedure are denoted with a "1" in the notes section of Table 8. Figure 28 shows a much more consistent performance during the inbound and outbound portions of the run, indicating the orientation of one or both vehicles has an effect on performance.

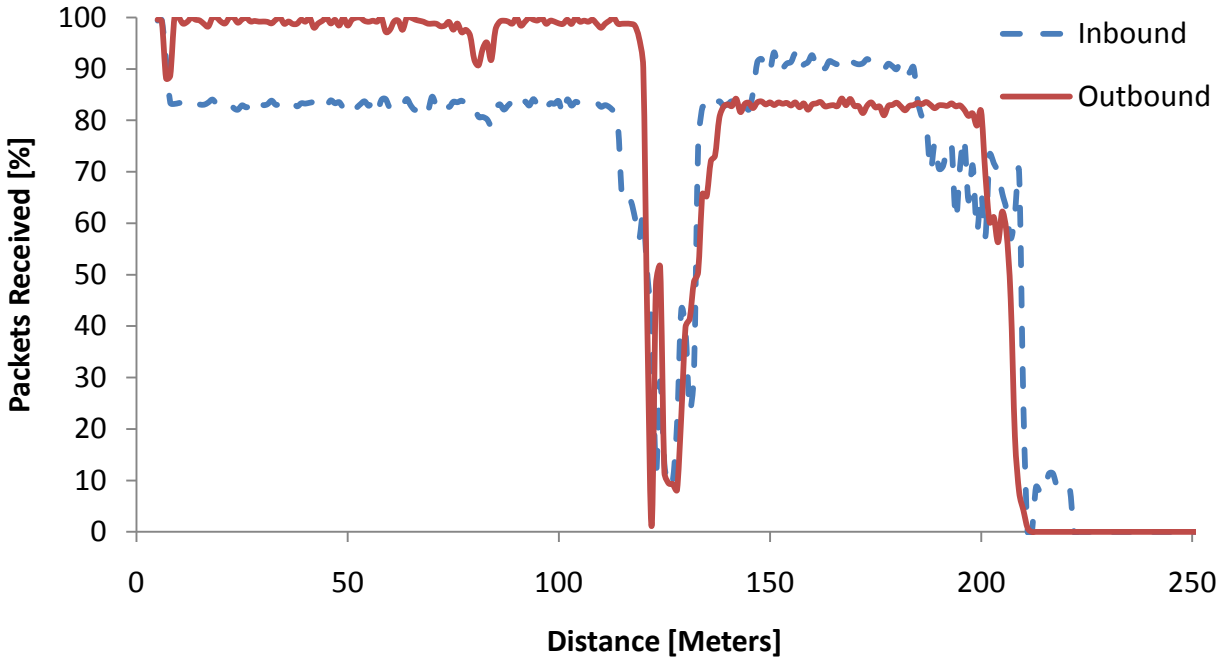


Figure 28. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters using a modified driving pattern where illustrating the similarity in performance between nodes moving closer (Inbound) to each other versus farther away (Outbound).

Further attempts were made to better understand the nature of this effect by producing a plot of performance versus transmission angle and distance. However, these plots did not produce useful information because they were sparsely populated with data and no clear trends could be observed.

Since the objective of this work is to demonstrate the potential performance of 802.11 networks when subjected to agricultural field conditions, the outbound data will be used in the following analyses. However, it should be noted that a thorough understanding of the effect of the vehicle on the transmission pattern of the wireless system should be conducted before evaluating a wireless network.

5.3 Performance of 802.11b Versus 802.11g

Figure 29 illustrates the difference in performance between an 802.11b and 802.11g network operating at comparable data rates. The 802.11b network is influenced by ground reflections as expected in the 195-meter range but otherwise provides consistent performance until 465 meters. The 802.11g network offers reliable performance up to approximately 170 meters with the exception of a drop in performance at 60-70 meters. At 170 meters, the network appears to be influenced by ground reflections and exhibits intermittent performance until 435 meters. Both protocols transmit data to nearly the same maximum distances, but 802.11b is much more consistent in its performance.

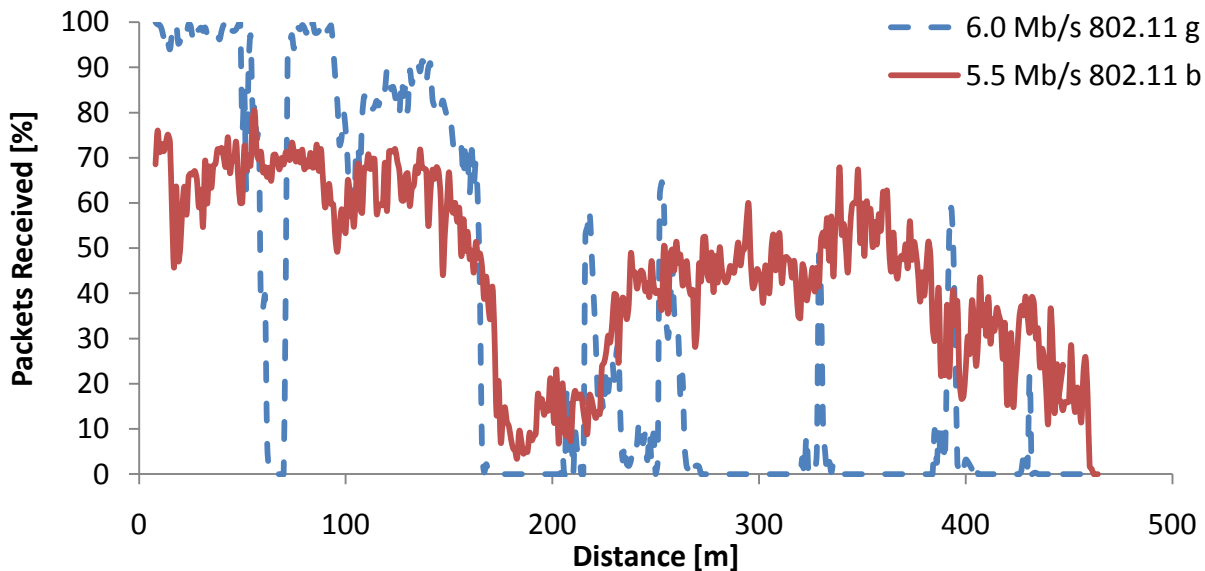


Figure 29. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and 802.11b at 5.5 Mbits/sec and an antenna height of 3.47 meters (Runs 3 and 8).

The 802.11b network is clearly more reliable at distances greater than 200 meters, but quantifying this performance difference is not achieved by measuring the maximum transmission distance. In order to distinguish between networks or segments of operation with erratic or consistent behavior, the concept of a reliability budget is introduced.

A reliability budget is a measure of how much performance is left in the network at a given distance. It can be defined as

$$RB(x) = \frac{\int_x^D PR(x)dx}{100} \quad (22)$$

where $PR(x)$ is the percentage of packets received as a function of distance between nodes, x , and D is the maximum transmission distance. Figure 30 shows the reliability budget for the same runs as in Figure 29. Many of the properties of each curve in Figure 29 can be observed as a different but related property in Figure 30. For example, Figure 30 shows the reliability budget value of 802.11b is greater than 802.11g at small distances which corresponds to the observation that the area under the 802.11b curve in Figure 29 is greater than the area under the 802.11g curve. Also notice the area of poor performance for 802.11g at about 65 meters in Figure 29 correlates to the instantaneous flat region at 65 meters on the corresponding curve in Figure 30.

There are two important properties associated with a reliability budget curve: slope and linearity. Figure 30 also displays the ideal or maximum achievable reliability budget as a straight dotted line with a slope that has a magnitude of 1. A reliability curve for a network that has any dropped packets will have a slope less than 1, with a larger slope indicating a more reliable system over the operating range. The more linear the curve is, the more consistent the system performs at that reliability level. An approximate slope was calculated by determining the slope for a line that intersects the reliability budget through the endpoints of the reliability curve. The linearity of the curve was determined by using Equation (23) to sum up the deviations of the reliability curve from the straight line approximation of the curve formed by drawing a line between the two end points of the reliability curve.

$$RD = \sqrt{\frac{\sum_{i=0}^{i=D} \{RB(d) - (RB(0) - RB_{slope} * d)\}}{D}} \quad (23)$$

In Equation (23), RD is the reliability deviation and RB_{slope} is the slope obtained when drawing a line between the two end points of the reliability curve.

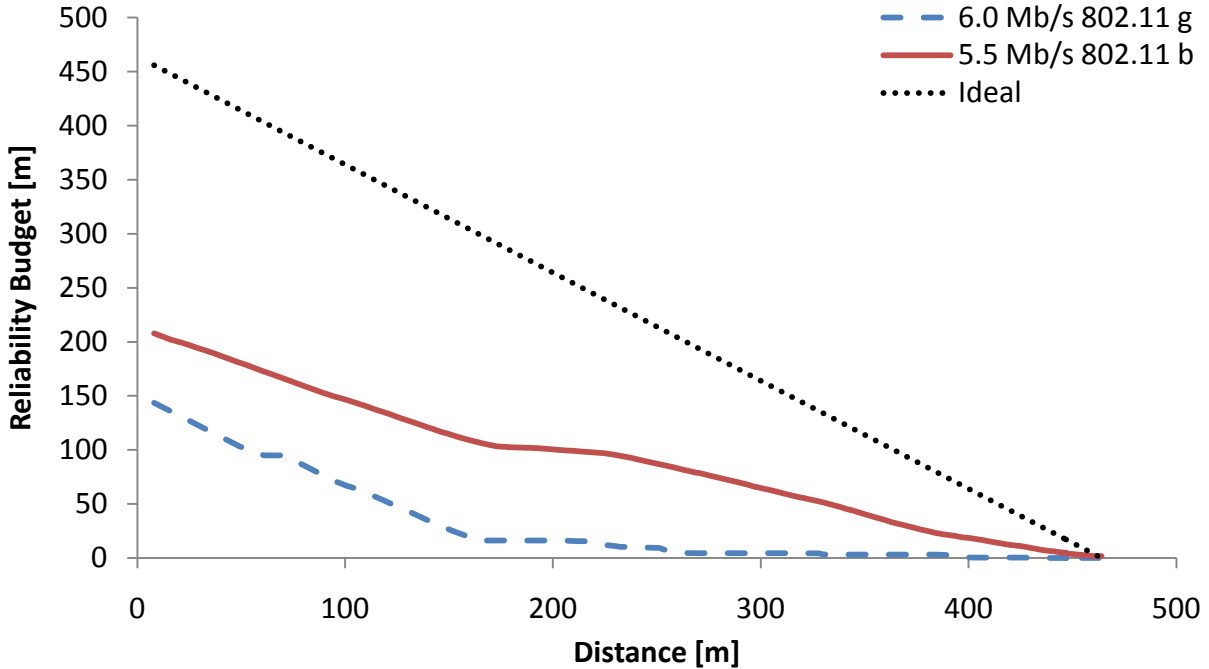


Figure 30. Plot of reliability budget versus distance using 802.11g at 6 Mbits/sec and 802.11b at 5.5 Mbits/sec and an antenna height of 3.47 meters (Runs 3 and 8).

Table 10 computes the performance statistics for both 802.11b and 802.11g systems operating at comparable data rates. Notice that 802.11b has a larger reliability budget slope, indicating an overall more reliable system, as well as a lower reliability budget deviation, indicating more consistent performance over the duration of the run.

Table 10. Performance statistics comparing 802.11b and 802.11g networks.

		Max Distance [meters]	Max Reliability Budget [m]	RB Slope [%/m]	RB Deviation [%]	Data Rate [Mb/s]
802.11 b	5.5 Mb/s	465	209.07	0.45	24.79	5.5
802.11 g	6.0 Mb/s	435	144.50	0.34	76.46	6.0

5.4 Effect of Data Rate on 802.11 Reliability

Table 11 lists the maximum distances achieved for the different configurations tested. Surprisingly, the trend for 802.11b protocols was that increasing the data rate did not have a

significant effect on the maximum distance at which the network would transmit data. However, the reliability budgets for 802.11b networks showed better results at lower data rates as illustrated by Figure 31. For 802.11g networks, there was a more defined inverse relationship where increasing data rates decreased the maximum distance at which the network would transmit data. However, Figure 32 illustrates that the reliability budget displayed more of a consistent bilinear trend, indicating robust performance for shorter distances and then inconsistent reliability at distances greater than that point. This supports the observations by Alexander et al. (2007) and Matolak (2008) that document the susceptibility of 802.11g in outdoor environments due to multipath effects. With increasing data rates, the amount of time between each symbol decreases, allowing the multipath effect to interfere with adjacent frames at closer distances.

Table 11. Maximum distance at which packets were received for the protocols tested.

		Max Distance [meters]	Max Reliability Budget [m]	RB Slope [%/m]	RB Deviation [%]	Data Rate [Mb/s]
802.11 b	1 Mb/s	447	347.96	0.79	16.67	1.0
	2 Mb/s	500	196.59	0.40	26.39	2.0
	5.5 Mb/s	465	209.07	0.45	24.79	5.5
802.11 g	6 Mb/s	435	144.50	0.34	76.46	6.0
	12 Mb/s	441	175.37	0.41	65.29	12.0
	18 Mb/s	158	102.83	0.69	12.11	18.0
	36 Mb/s	154	64.93	0.44	21.06	36.0
	54 Mb/s	129	27.02	0.22	23.19	54.0

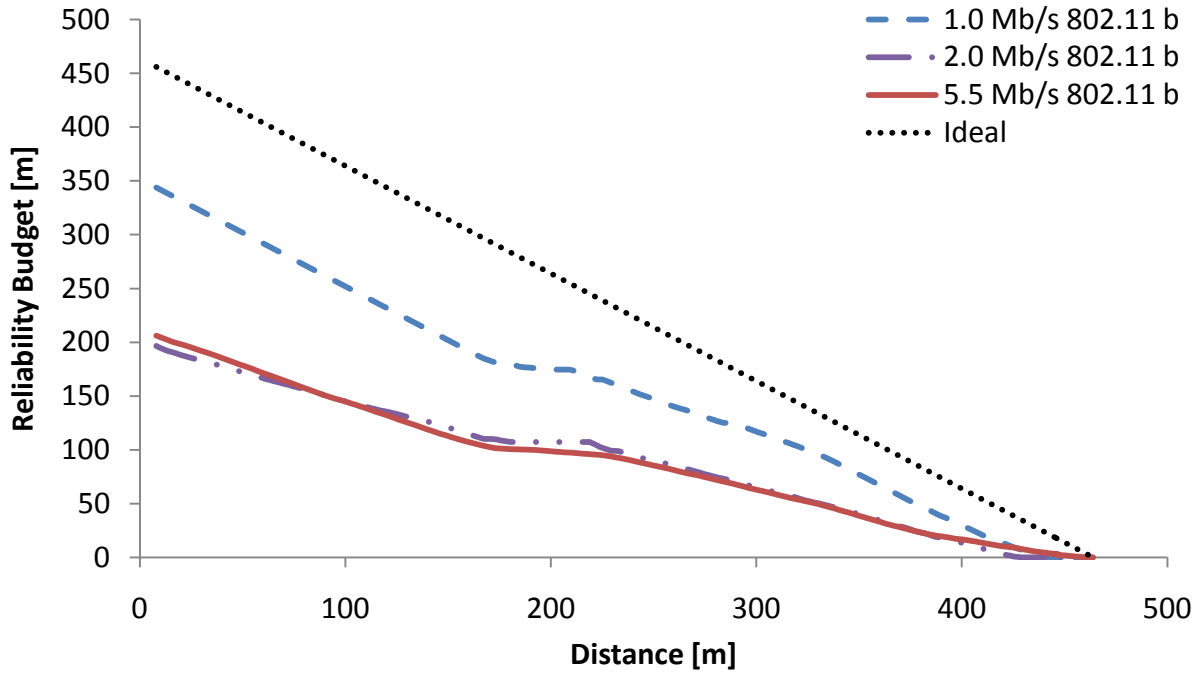


Figure 31. Plot of reliability budget versus distance for all 802.11b data rates using an antenna height of 3.47 meters.

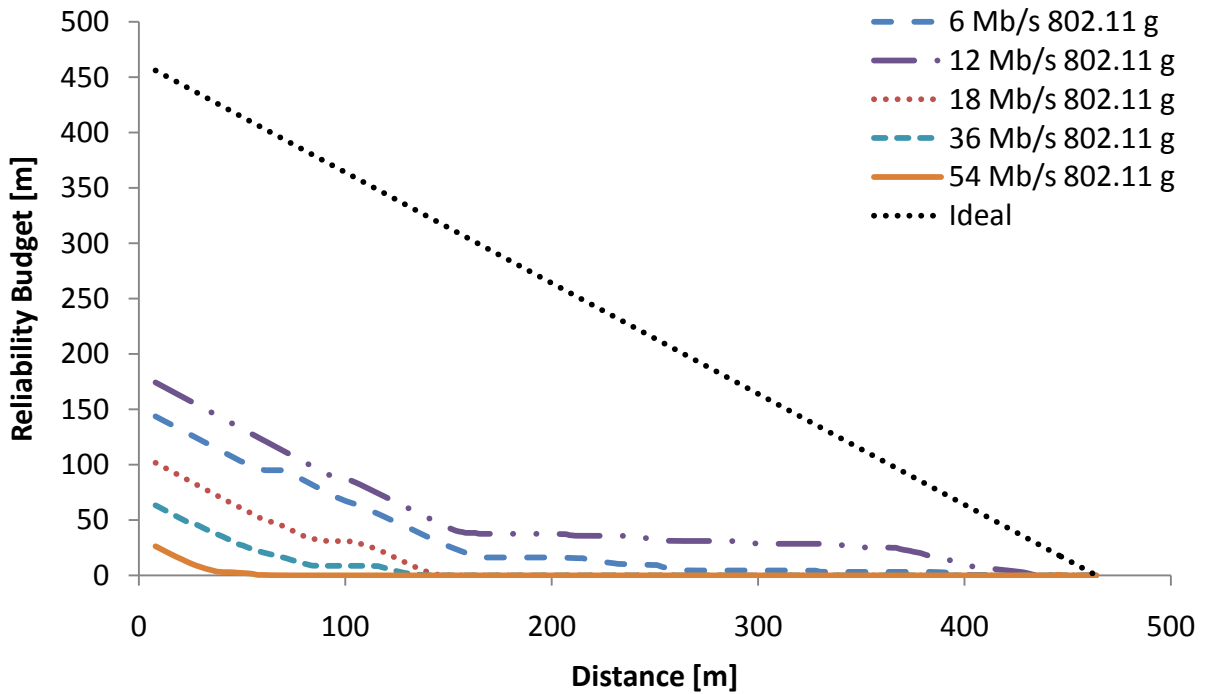


Figure 32. Plot of reliability budget versus distance for all 802.11g data rates using an antenna height of 3.47 meters.

5.5 Effect of Packets Size on 802.11 Reliability

Figure 33 displays the reliability versus distance for each packet size and is representative of a common run. Packet sizes of 15, 150, 500, 1000, and 1400 bytes usually followed a similar curve, while the reliability of the 2200 byte packet was visibly less at times. Two possible explanations exist for the reduced reliability of the largest packet. The first is that the 2200 byte packet is being split up into two smaller packets and broadcast over the network. The maximum frame size for an 802.3 network is 1488 bytes (IEEE, 2008) but the Standard states that when a packet is divided into multiple frames, it must be reassembled at the receiving device. With a maximum frame size for an 802.11 network of 2345 bytes (IEEE, 2007), the packet should be reassembled and broadcast as a single frame. In this case, if the packets were divided up into two 1100 byte frames, the reliability would be the squared value of the probability of a single 1100 byte packet making it across the network. The second explanation is that as packet size grows, there is a sharp degradation in reliability. It is beyond the scope of this work to determine the exact explanation for this behavior because it would involve obtaining proprietary information specific to the hardware that was used in this research.

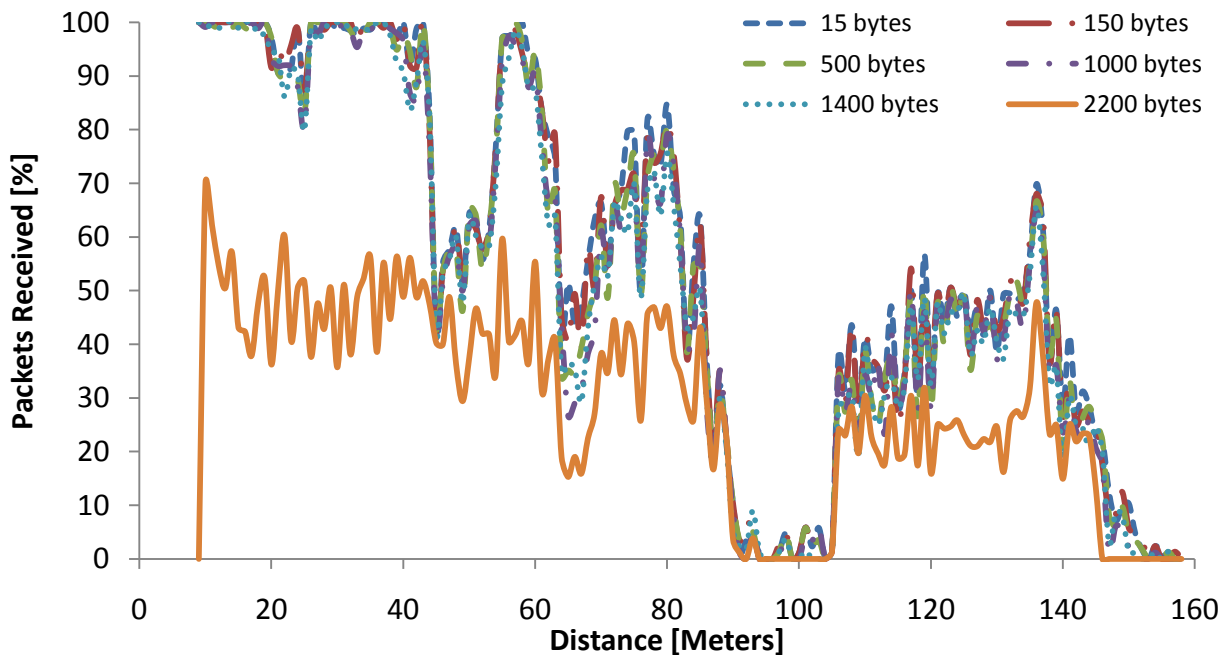


Figure 33. Plot of packets received versus distance using 802.11g at 18 Mbits/sec with an antenna height of 3.47 meters for all tested packet sizes (Run 5).

Figure 33 also illustrates the close relationship between the smaller packet sizes that were tested. One-way ANOVAs were completed using the following technique. For each distance interval, data was normalized between all packet sizes. The normalization process for each distance interval helped reduce the variation within a particular packet size. For example, if a particular packet size typically performed the best, it would likely be normalized to 100%, reducing the variance between performance measurements for that packet size across varying distances. After each distance interval was normalized, then two one-way ANOVAs were run, one to see if there were significant differences between any of the different-sized packets, and another to see if there were significant differences between any packet sizes of 15, 150, 500, 1000, and 1400 bytes.

For the first ANOVA that compared all six packet sizes, the results for every run were significant to a very high confidence level. For the second ANOVA that compared packet sizes of 15, 150, 500, 1000, and 1400 bytes, 16 of 18 runs had performance differences due to packet sizes at a 95% confidence. Table 12 summarizes the normalized mean packet reliability and variance for each packet size and presents the results of both of the ANOVA analyses for each run with the two shaded regions indicating results that are not significant. It was also observed that for each run, there was a consistent increase in normalized mean packet reliability with decreasing packet size. This relationship suggests that it might be beneficial to design a system utilizing an 802.11 network to transmit important data in small messages separate from transmissions of larger, less important data to increase the probability of transmission success.

Table 12. Results of two one-way ANOVA tests to determine if there were significant differences between packet sizes 1,2,3,4,5,6 and 1,2,3,4,5. The shaded regions denote analyses that are not statistically significant.

Run	AVG or VAR	Packet Size 1 (15 bytes)	Packet Size 2 (150 bytes)	Packet Size 3 (500 bytes)	Packet Size 4 (1000 bytes)	Packet Size 5 (1400 bytes)	Packet Size 6 (2200 bytes)	One Way ANOVA for Packet Sizes 1,2,3,4,5,6			One Way ANOVA for Packet Sizes 1,2,3,4,5		
								F value	F critical	P value	F value	F critical	P value
RUN 1	AVG	89.4	89.1	86.3	84.1	83.4	74.7	24.36	2.22	4.72E-24	7.09	2.38	1.13E-05
	VAR	447.5	392.8	505.8	520.4	539.0	763.3						
RUN 2	AVG	74.4	71.1	65.4	64.2	64.1	12.9	241.51	2.22	0.00E+0	9.12	2.38	2.62E-07
	VAR	1231.1	1178.2	1170.2	1162.0	1140.3	483.0						
RUN 3	AVG	51.6	51.3	48.8	48.0	48.1	26.0	20.47	2.22	4.29E-20	.61	2.38	6.53E-01
	VAR	2158.2	2154.2	2059.7	2044.6	2076.9	1379.4						
RUN 4	AVG	68.1	64.0	57.4	55.1	54.3	26.9	53.12	2.22	1.24E-52	8.53	2.38	7.88E-07
	VAR	1917.1	1888.1	1767.3	1787.0	1819.2	1099.5						
RUN 5	AVG	90.8	90.0	85.0	79.9	79.7	45.5	62.66	2.22	4.53E-56	6.02	2.38	9.04E-05
	VAR	577.3	585.8	657.2	863.3	816.3	582.4						
RUN 6	AVG	80.6	75.3	65.5	63.5	61.4	37.0	24.05	2.22	9.49E-23	6.8	2.38	2.22E-05
	VAR	1451.6	1440.1	1585.5	1545.3	1498.7	988.3						
RUN 7	AVG	54.9	42.1	31.7	29.1	28.5	21.3	10.65	2.23	6.74E-10	8.68	2.39	8.11E-07
	VAR	2405.6	2037.8	1668.3	1536.5	1393.0	965.0						
RUN 8	AVG	79.2	73.6	63.0	60.6	62.5	3.6	412.75	2.22	0.00E+0	31.55	2.37	8.56E-26
	VAR	1257.0	1281.9	1337.3	1338.6	1302.2	142.0						
RUN 9	AVG	96.4	92.9	86.2	86.0	87.2	13.0	1252.05	2.22	0.00E+0	30.81	2.38	1.56E-24
	VAR	52.8	89.2	319.0	257.6	199.3	325.5						
RUN 10	AVG	86.1	77.9	60.2	53.1	55.9	5.9	485.64	2.22	0.00E+0	116.41	2.38	1.84E-90
	VAR	738.1	805.9	819.7	945.9	861.5	269.0						
RUN 11	AVG	42.8	39.2	35.2	32.4	34.7	6.6	42.89	2.22	1.62E-42	3.8	2.38	4.38E-03
	VAR	2254.1	2015.3	1726.6	1563.9	1662.0	378.2						
RUN 12	AVG	72.6	67.5	59.5	56.1	57.5	6.5	111.17	2.22	0.00E+0	8.4	2.38	1.09E-06
	VAR	1781.2	1716.6	1484.2	1472.9	1519.7	107.9						
RUN 13	AVG	75.8	68.4	58.7	54.6	56.0	23.7	113.46	2.22	0.00E+0	27.44	2.38	2.45E-22
	VAR	1652.6	1602.0	1528.8	1508.1	1495.1	966.6						
RUN 14	AVG	83.6	78.7	69.3	66.8	67.2	17.6	235.19	2.22	0.00E+0	21.67	2.38	1.38E-17
	VAR	1191.8	1261.4	1367.9	1349.0	1249.7	460.9						
RUN 15	AVG	79.0	76.6	68.7	66.6	67.1	7.5	298.26	2.22	0.00E+0	11.99	2.38	1.20E-09
	VAR	1364.1	1339.9	1242.7	1252.0	1227.1	195.0						
RUN 16	AVG	79.7	78.6	74.6	73.1	71.2	45.2	26.76	2.22	6.76E-26	2.02	2.38	8.88E-02
	VAR	1546.0	1526.5	1520.8	1447.9	1449.2	975.3						
RUN 17	AVG	88.0	85.1	81.3	78.6	76.9	45.7	83.63	2.22	4.86E-80	7.46	2.38	5.96E-06
	VAR	984.6	956.8	945.3	944.3	937.1	966.5						
RUN 18	AVG	93.7	86.3	74.0	69.9	69.6	21.7	442.14	2.22	0.00E+0	101.39	2.38	8.12E-80
	VAR	261.0	418.0	629.4	713.6	709.3	1384.9						

CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

A total of 18 runs were completed for the evaluation of an 802.11b/g wireless network in a realistic in-field agricultural environment. Multiple conclusions can be drawn from this performance evaluation.

Consistent with results from Alexander et al. (2007) and Matolak (2008), the 802.11b network performed much better in the outdoor environment by transmitting data more reliably and farther than the 802.11g network. A new parameter, called a reliability budget, was created to help quantify performance differences between wireless networks. Using a plot of 802.11g reliability budgets versus distance, a bilinear trend was identified indicating a high reliability region, usually at small distances between nodes, and a region with less reliability, at larger distances between nodes. Increasing 802.11g data rates decreased the distance over which the network would reliably transmit, but increasing 802.11b data rates had little effect on maximum transmission distance but decreased the overall reliability of the network.

For packets between 15 and 1400 bytes in length, small but statistically significant decreases in reliability were observed with increasing packet size. For the largest packet size of 2200 bytes, more notable reliability decreases were observed.

The network performance was influenced by the angle of the transmitted wave relative to the tractor orientation. The exact reason for this could not be determined, but data considered to be affected by this were not used in this analysis.

Finally, performance degradation due to signal reflections off of the soil surface could be observed at distinct distances between nodes. This observation confirms the nearly ideal reflective properties of the soil and illustrates the need to create a network that is not easily affected by these reflections.

The following recommendations are made for future investigations into in-field agricultural networks:

1. Evaluate the performance of 802.11n under the same conditions as this work. 802.11n uses OFDM modulation techniques similar to 802.11g, which can have a negative impact

on performance, but the addition of MIMO technology should help improve performance, especially in multipath environments. A thorough examination of this technology and how it compares to 802.11b and 802.11g would be beneficial.

2. Investigate other possible solutions to mitigate performance degradation due to ground signal reflections. Potential solutions might include: a) using a radio with multiple antennas and mounting one antenna above the other; b) placing a ground plane at the base of the antenna; and c) integrating a ground plane structure into the vehicle roof. As previously mentioned, these effects will also be present on unlevel ground but in a less identifiable pattern.
3. Evaluate influences of tractor structure on the antenna pattern. A test should be specifically designed to collect data that will yield a plot of reliability as a function of distance and angle.

In conclusion, 802.11 networks have a promising future for use in an in-field agricultural environment. The reliable performance over short distances already makes this networking technology viable for short-range applications while offering the possibility of extending the network across the field. With continued improvements and new technology, 802.11 will eventually find its way from consumer and industrial environments into agricultural fields.

REFERENCES

- Alexander, P., D. Haley, and A. Grant. 2007. Outdoor Mobile Broadband Access with 802.11. *IEEE Communications Magazine* 45(11): 108-114.
- Behzad, A. 2008. *Wireless LAN Radios: System Definition to Transistor Design (IEEE Series on Digital & Mobile Communication)*. Hoboken, NJ.: John Wiley and Sons.
- Bergamo, P., D. Maniezzo, K. Yao, M. Cesana, G. Pau, M. Gerla, and D. Whiteman. 2003. IEEE 802.11 wireless network under aggressive mobility scenarios. In *Proc. International Telemetry Conference*, Las Vegas, NV.: International Foundation for Telemetry.
- Carvalho, F. B. S. 2008. Challenges for Infotainment Expansion in Automotive Market. SAE Brazil Paper No. 2008-36-0303. São Paulo, Brazil: SAE International.
- Caterpillar. 2010. Fleet Management Solutions: Product Link™. Peoria, IL.: Caterpillar. Available at: www.cat.com/technology/fleet-management-solutions. Accessed 24 May 2010.
- Deere and Company. 2010. Information and Logistics: JDLink™. Moline, IL.: John Deere Co. Available at: www.deere.com/en_US/ProductCatalog/FR/series/ams/info_logistics/info_logistics.html. Accessed 24 May 2010.
- Deere and Company. 2010. Operator's Manual StarFire iTC and RTK. OMPC21514 Issue E9. Moline, IL.: John Deere Co. Available at: stellarsupport.deere.com/en_US/support/pdf/om/en/OMPC21514_StafireiTC_RTK.pdf. Accessed 24 May 2010.
- FCC. 2009. FCC CFR 47 Part 15. Available at: www.fcc.gov. Accessed 16 June 2010.
- Gass, R., J. Scott, and C. Diot. 2006. Measurements of In-Motion 802.11 Networking. In *Proc. 7th IEEE Workshop on Mobile Computing Systems & Applications*, 69-74. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Griffin, T. 2009. Whole-farm Benefits of GPS-enabled Navigation Technologies. ASABE Paper No. 095983. St. Joseph, MI.: ASABE.
- Hansen, A. C., R. H. Hornbaker, and Q. Zhang. 2003. Monitoring and Analysis of in-field grain handling operations. ASAE Paper No. 701P1103. St. Joseph, MI.: ASABE.
- Heegard, C., J.T. Coffey, S. Gummadi, P.A. Murphy, R. Provencio, E.J. Rossin, S. Schrum, and M.B. Shoemake. 2001. High performance wireless Ethernet. *IEEE Communications Magazine* 39(11): 64-73.

- IEEE, 1985. IEEE Standards for Local Area Networks: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. *ANSI/IEEE Std 802.3-1985*, 1-144.
- IEEE, 1995. IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T (Clauses 21-30). *IEEE Std 802.3u-1995 (Supplement to ISO/IEC 8802-3: 1993; ANSI/IEEE Std 802.3, 1993 Edition)*, 1-398.
- IEEE, 1997. IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-1997*, 1-445.
- IEEE, 2000. Supplement to IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks-Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. *IEEE Std 802.11b-1999*, 1-90.
- IEEE, 2003. IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)*, 1-67.
- IEEE, 2007. IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, 1-1184.
- IEEE, 2008. IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks--Specific Requirements Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Section One. *IEEE Std 802.3-2008 (Revision of IEEE Std 802.3-2005)*, 1-597.
- IEEE, 2009. IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-*

- 2008, *IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009*), 1-502.
- Ipatov, V. P. 2005. *Spread Spectrum and CDMA Principles and Applications*. West Sussex, England.: John Wiley and Sons, Ltd.
- ISO/IEC 7498-1. 1994. *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1-23.
- Jiang, D., and L. Delgrossi. 2008. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In *Proc. Vehicular Technology Conference, 2008*, 2036-2040. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Lathi, B. P. 1965. *Signals, Systems and Communication*. Etobicoke, Canada: John Wiley and Sons, Ltd.
- Lee, W. C. Y. 1998. *Mobile Communications Engineering: Theory and Applications*. New York, NY.: The McGraw-Hill Companies, Inc.
- Li, Y., and G. Stüber. 2006. *Orthogonal Frequency Division Multiplexing For Wireless Communications*. New York, NY.: Springer Science and Business Media, Inc.
- Logical Link Control. 1984. ANSI/IEEE Std 802.2.
- Lupini, C. A. 2010. In-Vehicle Networking Technology for 2010 and Beyond. SAE International Paper No. 2010-01-0687. Warrendale, PA.: SAE International.
- Matolak, D.W. 2008. Channel Modeling for Vehicle-To-Vehicle Communications. *IEEE Communications Magazine* 46(5):76-83.
- McCune, E. 2000. DSSS vs. FHSS narrowband interference performance issues. *www.rfdesign.com*. September 2000: 90-104. Available at: <http://mobiledevdesign.com/images/archive/0900McCune90.pdf>. Accessed 5 June 2010.
- McCurdy, P., and I. Sharp. 2006. Wi-Fi... Why Now? Exploring New Wireless Technologies for Industrial Applications. ISA Paper. Durham, NC.: ISA.
- Olexa, R. 2005. *Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations*. Oxford, England: Newnes, an imprint of Elsevier, Inc.
- Ott, J., and D. Kutscher. 2004. Drive-thru Internet: IEEE 802.11b for ‘automobile’ users. In *Proc. INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 373. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Perahia, E. 2008. IEEE 802.11n Development: History, Process, and Technology. *IEEE Communications Magazine* 46(7): 48-55.

- Pickholtz, R. L., D. L. Schilling, and L. B. Milstein. 1982. Theory of Spread-Spectrum Communications—A Tutorial. *IEEE Transactions on Communications* 30(5): 855-884.
- Postel, J. 1980. RFC-768: User Datagram Protocol. *Request For Comments*.
- Postel, J. 1981. RFC-791: Internet Protocol. *Request For Comments*.
- Postel, J. 1981. RFC-793: Transmission Control Protocol. *Request For Comments*.
- Rappaport, T. S. 2002. *Wireless Communications Principles & Practice*. Upper Saddle River, NJ.: Prentice Hall PTR.
- Reed, S. 2009. Physical Aspects of Applying Wireless Sensors: Short range, UHF radio waves and antennas in natural environments. *ASABE Resource* (1): 8-11.
- Reid, J. F. 2004. Mobile Intelligent Equipment for Off-road Environments. ASAE Paper No. 701P1004. St. Joseph, MI.: ASAE.
- Riblett, L.E., and E. L. Witzke. 2009. Findings on the suitability of 802.11 for highly mobile broadband networks. In *Proc. Military Communications Conference, 2009*, 1-7. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Seybold, J. S. 2005. *Introduction to RF Propagation*. Hoboken, N.J.: John Wiley and Sons, Inc.
- Singh, J.P., N. Bambos, B. Srinivasan, and D. Clawin. 2002. Wireless LAN performance under varied stress conditions in vehicular traffic scenarios. In *Proc Vehicular Technology Conference, 2002*, 743-747. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Stallings, W. 1987. *Handbook of Computer-Communications Standards – The Open Systems Interconnection (OSI) Model and OSI-Related Standards*. Volume 1. New York, NY.: Macmillan Publishing Company.
- Tonguz, O. K., F. Bai, and C. U. Saraydar. 2010. Vehicular networks. *Ad Hoc Networks* (8): 457-461.
- Topcon. 2010. Telematic Products: Topcon Tierra™. Livermore, Cal.: Topcon Positioning System, Inc. Available at: <http://www.topcontierra.com/products>. Accessed 24 May 2010.
- Trimble. 2010. Fleet and Asset Management Solution: VisionLink™. Sunnyvale, Cal.: Trimble Navigation Limited. Available at: investor.trimble.com/releasedetail.cfm?ReleaseID=460953. Accessed 24 May 2010.
- Warren, J.C. 2009. Ethernet/IP Applications for Electrical Industrial Systems. In *Proc. Industry Applications Society Annual Meeting, 2009*, 1-5. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.

- Wellens, M., B. Westphal, and P. Mahonen. 2007. Performance Evaluation of IEEE 802.11-based WLANs in Vehicular Scenarios. In *Proc. Vehicular Technology Conference, 2007*, 1167-1171. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.
- Yong S., Q. Zou, and Z. Liu. 2009. Performance Evaluation of IEEE802.11-Based Ad-Hoc Wireless Networks in Vehicular Environments. In *Proc. Wireless Communications, Networking and Mobile Computing Conference, 2009*, 1-4. Los Alamitos, CA.: Institute of Electrical and Electronics Engineers.

APPENDIX A: ENGENIUS™ 802.11 RADIO CONFIGURATION

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- ◉ **Bridge:** Client Bridge provides connectivity between two wired LAN segments, and is used in point-to-point or point-to-multipoint configurations.
- **Bridge Router:** Client Router designed to connect a small number of wireless nodes to a single device for LAN and WLAN connectivity to another network.
- **AP:** Access Point is probably the most common wireless LAN device with which you will work as a wireless LAN administrator. Access point provides clients with a point of access into a network.

Figure 34. Operation mode setup for Engenius™ 802.11 radio.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.1.254"/>
DHCP:	<input type="text" value="Disabled"/> ▾
DHCP Client Range:	<input type="text" value="192.168.1.100"/> -
	<input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>

Figure 35. LAN interface setup for Engenius™ 802.11 radio.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band: 2.4 GHz (B+G)

SSID:

Channel: 1

Associated Clients:

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

Figure 36. Basic wireless settings for 802.11 radio configured as access point.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System	<input type="radio"/> Shared Key	<input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/>	(256-2346)	
RTS Threshold:	<input type="text" value="2347"/>	(0-2347)	
Beacon Interval:	<input type="text" value="100"/>	(20-1024 ms)	
Ack Timeout:	<input type="text" value="0"/>	(0-255 x 4 us)	
	Note: Ack Timeout default CCK:316 us OFDM:72 us.		
Data Rate:	<input type="text" value="Auto"/>		
Output Power Level(OFDM):	<input type="text" value="High"/>		
Output Power Level(CCK):	<input type="text" value="High"/>		
Preamble Type:	<input checked="" type="radio"/> Long Preamble	<input type="radio"/> Long & Short Preamble	
Broadcast SSID:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
IAPP:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
802.11g Protection:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
User Isolation:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	
QoS(WMM):	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	

Figure 37. Advanced wireless settings for 802.11 radio configured as access point.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	<input type="text" value="2.4 GHz (B+G)"/>
Network Type:	<input type="text" value="Infrastructure"/>
SSID:	<input type="text" value="EnGenius"/>
Desired BSSID:	<input type="text" value="000000000000"/>
Channel:	<input type="text" value="1"/>
<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	
SSID of Extended Interface:	<input type="text"/>

Figure 38. Basic wireless settings for 802.11 radio configured as bridge.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type: Open System Shared Key Auto

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Ack Timeout: (0-255 x 4 us)

Note: Ack Timeout default CCK:316 us OFDM:72 us.

Data Rate: ▾

Output Power Level(OFDM): ▾

Output Power Level(CCK): ▾

Preamble Type: Long Preamble Long & Short Preamble

Transparent Bridge: Enabled Disabled

Figure 39. Advanced wireless settings for 802.11 radio configured as bridge.


```

DCB SPprop; // Properties of serial port
COMMTIMEOUTS Sptimeouts; // Timeout properties so the serial
port does not hang
char file_name[256]; // Name of file to receive //
#define SPBUFSIZE 1000 // Serial port buffer size
char sp_buf[SPBUFSIZE]; // Serial port buffer
#define PBUFSIZE 1000 // Parse buffer size
char input_buf[PBUFSIZE]; // Parsing buffer for serial port
short int bufidx = 0; // index into parse buffer
char sp_input_buf[PBUFSIZE]; // Intermediate serial port buffer

//GPS variables
struct GPS
{
    unsigned char    diff_type;
    float            altitude, mph, seconds_today;
    unsigned char    differential;
    double           latitude;
    double           longitude;
    char             hour, min, second, secondX10, day, month, year;
    int              full_year;
    char             new_data;
};
struct GPS Position;

//General Server / Client Socket Variables
#define BUFFER_SIZE 5000
#define PORT_OFFSET 22349 //this number was chosen so I could
get through the firewall on all the pc's
WSADATA w; // Used to open windows
connection */

//Receiving Server / Client Socket Variables
//In this case we are the receiving server and the other computer is the
sending client
unsigned short server_port_number; // Port number to use */
int client_length; // Length of client struct */
SOCKET ssd; // Socket descriptor of
server */
struct sockaddr_in server; // Information about the server */
char rbuffer[BUFFER_SIZE]; // Where to store received data */
struct hostent *hp; // Information about this
computer */
char host_name[256]; // Name of the server */

//Sending Server / Client Socket Variables
//In this case we are the sending client and the other computer is the
receiving server
unsigned short client_port_number; // Port number to use */
SOCKET rsd; // Socket descriptor of
server */
struct sockaddr_in rserver; // Information about the receiving
server */

```

```

struct sockaddr_in sclient;          /* Information about the sending
client */
char sbuffer[BUFFER_SIZE];         /* Where to store data to send*/
int tx_packet_length;              /* Length of the current packet
being sent*/
struct hostent *hp;                /* Information about this
computer */
char host_name[256];               /* Name of the server */

//Timing variables
LARGE_INTEGER ticksPerSecond, tick1, tick2, tick3, tick4, tick5;
signed long long int pktTXtime = 0;

//Packet statistics
unsigned long int sequence_num = 0;
// used to uniquely identify each packet
unsigned long int total_packet_count = 0, total_packets_received = 0;
// total packets out and in
unsigned long long int total_bytes_sent = 0, total_bytes_received = 0;
// total bytes out and in
unsigned int
packet_lengths[NUM_PKT_LEN]={PKT_0,PKT_1,PKT_2,PKT_3,PKT_4,PKT_5}; // array
of packets lengths
unsigned int packets_sent[NUM_PKT_LEN]={0,0,0,0,0,0};
// cumulative packets sent for each size of packet
unsigned int packets_recv[NUM_PKT_LEN]={0,0,0,0,0,0};
// cumulative packets received for each size of packet
unsigned int st_packets_sent[NUM_PKT_LEN]={0,0,0,0,0,0};
// short term packets sent for each size packet
unsigned int st_packets_recv[NUM_PKT_LEN]={0,0,0,0,0,0};
// short term packets received for each size packet
unsigned char lengthptr = 0;
// variable to server as pointer into these arrays

//Logging
FILE *fFileTX, *fFileRX;          // File pointers
char fnTX[200], fnRX[200];       // File name character arrays
int first_packet_received = 0;    // Flag that tells
application to start sending data
int send_start = 0, send_quit = 0; // Flags used to trigger start and
stop of other application

//temps
unsigned char u8tmp1;
signed char i8tmp1;
unsigned short int u16tmp1;
signed short int i16tmp1;
unsigned long int u32tmp1;
signed long int i32tmp1, i32tmp2;
short int i,j,k,n;
DWORD Error;

////////////////////
//Function Prototypes//
////////////////////
void set_up_serial_port(void);
void ParseNMEALine(char *);

```

```

int      CheckChecksum(char * GPSbuf);
void    set_up_UDP_server(void);
void    set_up_UDP_client(void);
void    make_master_packet(void);
void    open_log_files(void);

int main(int argc, char **argv)
{
    /****Get Inputs***/
    printf("Enter the IP address of the receiving device:\r\n");
    scanf("%i.%i.%i.%i", &a1, &a2, &a3, &a4);
    printf("Enter the data rate in Mbit/s:\r\n");
    scanf("%u",&datarate);
    if (datarate > 6)
    {
        act_data_rate = 6; //cap data rate to 6MByte/sec
    }
    else
    {
        act_data_rate = datarate;
    }
    act_data_rate *= (1000000/8); //convert data rate to MByte/sec
    printf("Enter the COM port you want NMEA to come in on:\r\n");
    scanf("%i",&COMport);
    printf("Enter the Antenna gain in dB:\r\n");
    scanf("%i",&antenna_gain);

    /****Set Up Serial Port***/
    set_up_serial_port(); //enables reception of GPS messages
    set_up_UDP_server(); //enables UDP server to listen and log oncoming
messages
    set_up_UDP_client(); //enables UDP client to send and log data
packets
    make_master_packet(); //populate the big blob of data to be sent
    open_log_files(); //get ready to write data

    // get the high resolution counter's accuracy
    QueryPerformanceFrequency(&ticksPerSecond);
    // what time is it?
    QueryPerformanceCounter(&tick5);
    QueryPerformanceCounter(&tick1);
    tick2.QuadPart = 0;

    while(1)
    {
        //make sure we are not supposed to quit
        if(kbhit())
        {
            in_char[0] = getch();
            in_char[1] = 0;
            if( (in_char[0] == '\r') || (in_char[0] == '\n') )
            {
                if(!strcmp(input_buf, "quit"))
                {
                    send_quit = TRUE;
                }
                if(!strcmp(input_buf, "start"))

```

```

        {
            send_start = TRUE;
        }
        input_buf[0] = 0;
    }
    else
    {
        strcat(input_buf, in_char);
    }
}

//see if new GPS data has arrived
ReadFile(SPhandle, (void *)sp_buf, SPBUFSIZE, &bytes_received,
NULL);
if(bytes_received)
{
    i=0;
    while(bytes_received)
    {
        if(sp_buf[i] == '$')
        {
            bufidx = 0;
        }
        sp_input_buf[bufidx] = sp_buf[i];
        if( (sp_buf[i] == '\r') || (sp_buf[i] == '\n') )
        {
            sp_input_buf[bufidx] = 0; //terminate the
string

            if(bufidx > 0)
            {
                ParseNMEALine(sp_input_buf);
                Position.seconds_today = (float)(
Position.secondX10 / 10.0 + Position.second + Position.min*60 +
Position.hour* 3600);
            }
            bufidx = 0;
        }
        else
        {
            bufidx++;
        }
        i++; bytes_received--;
    }
}

//see if new UDP data has arrived
bytes_received = recv(ssd, rbuffer, BUFFER_SIZE, 0);
if(bytes_received != -1)
{
    send_start = FALSE;
    first_packet_received = TRUE;
    if(bytes_received == 6)
    {
        if(!strcmp(rbuffer, "Start"))

```

```

        {
            pktTXtime=0;
        }
    }
else if(bytes_received == 5)
{
    if(!strcmp(rbuffer,"Quit"))
    {
        break;
    }
}
else
{
    total_bytes_received += bytes_received;
    total_packets_received++;

    fprintf(fFileRX,"%s,%d,%.7f,%.7f,%.1f,%.1f\r\n",rbuffer,bytes_received,
Position.latitude,Position.longitude,Position.mph,Position.seconds_today);
    for(i=0;i<NUM_PKT_LEN;i++)
    {
        if(packet_lengths[i] == bytes_received)
        {
            break;
        }
    }
    if(i!=NUM_PKT_LEN)
    {
        packets_rcv[i]++;
        st_packets_rcv[i]++;
    }
}
}
QueryPerformanceCounter(&tick2);
if( ((tick2.QuadPart - tick1.QuadPart) > pktTXtime ) &&
(first_packet_received == TRUE) && (!send_quit) )
{
    lengthptr = (unsigned char) total_packet_count %
NUM_PKT_LEN;
    tx_packet_length = packet_lengths[lengthptr];

    i32tmp1 = sendto(rsd,sbuffer,tx_packet_length,0,(struct
sockaddr *)&rserver,client_length);

    fprintf(fFileTX,"%u,%u,%.7f,%.7f,%.1f,%.1f\r\n",sequence_num,tx_packet_
length,Position.latitude,Position.longitude,Position.mph,Position.seconds_tod_
ay);

    packets_sent[lengthptr]++;
    st_packets_sent[lengthptr]++;

    tick1.QuadPart = tick2.QuadPart;
    pktTXtime = tx_packet_length * ticksPerSecond.QuadPart /
(act_data_rate);
    pktTXtime *= (100 / NWORK_LOADING);

    if(lengthptr == (NUM_PKT_LEN - 1) )
    {

```

```

        sequence_num++;
        sprintf(sbuffer, "%d", sequence_num);
    }
    total_packet_count++;
    total_bytes_sent+= tx_packet_length;
}

QueryPerformanceCounter(&tick3);
//check to see if one second has elapsed since the last time this
was done
if((tick3.QuadPart - tick5.QuadPart) > ticksPerSecond.QuadPart )
{
    QueryPerformanceCounter(&tick5);
    if(input_buf[0] != 0)
    {
        printf("%s\r", input_buf);
    }
    else if (send_quit)
    {
        rbuffer[0]='Q';
        rbuffer[1]='u';
        rbuffer[2]='i';
        rbuffer[3]='t';
        rbuffer[4]=0;
        sendto(rsd, rbuffer, 5, 0, (struct sockaddr
*)&rserver, client_length);
        send_quit++;
        printf("Sending quit command to other unit\r\n");
        if(send_quit > 6)
        {
            break;
        }
    }
    else if (send_start)
    {
        rbuffer[0]='S';
        rbuffer[1]='t';
        rbuffer[2]='a';
        rbuffer[3]='r';
        rbuffer[4]='t';
        rbuffer[5]=0;
        sendto(rsd, rbuffer, 6, 0, (struct sockaddr
*)&rserver, client_length);
        printf("Sending start command to other unit\r\n");
    }
    else if( !send_start && !first_packet_received )
    {
        printf("Waiting for start command\r\n");
    }
    else if( (Position.new_data == FALSE) ||
(Position.longitude > -88.0 ) || (Position.longitude < -89.0 ) )
    {
        printf("Check GPS or COM port!\r\n");
    }
    else

```

```

        {
            printf("INST RX%:\t");
            for(i=0; i<NUM_PKT_LEN; i++)
            {
                if(st_packets_recv[i] > st_packets_sent[i])
                {
                    st_packets_recv[i] = st_packets_sent[i];
                }
                if( (st_packets_recv[i] + 1) ==
st_packets_sent[i])
                {
                    st_packets_recv[i]++;
                }
                printf("%d\t", (st_packets_recv[i] * 100 /
st_packets_sent[i]));
                st_packets_recv[i] = st_packets_sent[i] = 0;
            }
            printf("TOT RX%:\t");
            for(i=0; i<NUM_PKT_LEN; i++)
            {
                if(packets_recv[i] > packets_sent[i])
                {
                    packets_recv[i] = packets_sent[i];
                }
                printf("%d\t", (packets_recv[i] * 100 /
packets_sent[i]));
            }
            printf("\r\n");
        }
        Position.new_data = FALSE;
    }
    //print out ending statistics
    printf("total packets sent = %lu\r\ntotal bytes sent = %llu\r\ntotal
bytes received = %llu\r\ntotal packets received = %lu\r\n",
        total_packet_count, total_bytes_sent, total_bytes_received,
total_packets_received);

    //****clean up everything****//

    CloseHandle(SPhandle); //shut serial port
    closesocket(ssd); //get rid of the server socket
    closesocket(rsd); //get rid of the client socket
    fclose(fFileTX); //shut the TX log file
    fclose(fFileRX); //shut the RX log file
    WSACleanup();
}
void open_log_files(void)
{
    int erropen;
    sprintf(fnTX, "C:\\%u_%u_%u_TX.csv", datarate, (client_port_number%2), ante
nna_gain);
    erropen = fopen_s(&fFileTX, fnTX, "w" );
    if (erropen > 0 )
    {
        printf("FILE %s NOT OPENED \r\nTERMINATING PROGRAM", fnTX);
    }
}

```

```

        exit(0);
    }
    fprintf(fFileTX,"PN, PL, LAT, LON, SPD, TIME\r\n");
    //PN is packet number
    //PL is packet length
    //LAT is latitude
    //LON is longitude

    sprintf(fnRX,"C:\\%u_%u_%u_RX.csv",datarate, (server_port_number%2), ante
nna_gain);
    erropen = fopen_s(&fFileRX, fnRX, "w" );
    if (erropen > 0 )
    {
        printf("FILE %s NOT OPENED \r\nTERMINATING PROGRAM", fnRX);
        exit(0);
    }
    fprintf(fFileRX,"PN, PL, LAT, LON, SPD, TIME\r\n");
}
void make_master_packet(void)
{
    unsigned int i;

    srand( (unsigned)time( NULL ) );
    for(i=0; i<BUFFER_SIZE; i++)
    {
        sbuffer[i] = (unsigned char)(rand() & 0xFF);
    }
    sprintf(sbuffer,"%d",sequence_num);
}

void set_up_UDP_server(void)
{
    if (WSAStartup(0x0202, &w) != 0)
    {
        fprintf(stderr, "Could not open Windows connection.\n");
        exit(0);
    }
    ssd = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
    if (ssd == INVALID_SOCKET)
    {
        fprintf(stderr, "Could not create socket.\n");
        WSACleanup();
        exit(0);
    }
    gethostname(host_name, sizeof(host_name));
    hp = gethostbyname(host_name);

    /* Check for NULL pointer */
    if (hp == NULL)
    {
        fprintf(stderr, "Could not get host name.\n");
        closesocket(ssd);
        WSACleanup();
        exit(0);
    }
    /* Clear out server struct */
    memset((void *)&server, '\0', sizeof(struct sockaddr_in));
}

```



```

i = 0;

/* Assign the address */
server.sin_addr.S_un.S_un_b.s_b1 = hp->h_addr_list[i][0];
server.sin_addr.S_un.S_un_b.s_b2 = hp->h_addr_list[i][1];
server.sin_addr.S_un.S_un_b.s_b3 = hp->h_addr_list[i][2];
server.sin_addr.S_un.S_un_b.s_b4 = hp->h_addr_list[i][3];

server_port_number = hp->h_addr_list[i][3] + PORT_OFFSET;

server.sin_port = htons(server_port_number);
server.sin_family = AF_INET;

if (bind(ssd, (struct sockaddr *)&server, sizeof(struct sockaddr_in))
== -1)
{
    fprintf(stderr, "Could not bind name to socket.\n");
    closesocket(ssd);
    WSACleanup();
    exit(0);
}
else
{
    printf("Receiving Server Socket bound!\r\n");
}

i32tmp2 = sizeof(i32tmp1);

if (getsockopt(ssd, SOL_SOCKET, SO_RCVTIMEO, (char*)&i32tmp1, &i32tmp2)
!= SOCKET_ERROR) {
    printf("Receive Time Value: %ld\n", i32tmp1);
}
i32tmp1 = RX_BLOCK_TIME;

if (setsockopt(ssd, SOL_SOCKET, SO_RCVTIMEO, (char*)&i32tmp1, i32tmp2)
!= SOCKET_ERROR) {
    printf("Set Receive Time Value: %ld\n", i32tmp1);
}

if (getsockopt(ssd, SOL_SOCKET, SO_RCVTIMEO, (char*)&i32tmp1, &i32tmp2)
!= SOCKET_ERROR) {
    printf("Checked Receive Time Value: %ld\n", i32tmp1);
}
if (getsockopt(ssd, SOL_SOCKET, SO_MAX_MSG_SIZE, (char*)&i32tmp1,
&i32tmp2) != SOCKET_ERROR) {
    printf("Max Message Length: %ld\n", i32tmp1);
}

u32tmp1 = TRUE;
i32tmp1 = ioctlsocket(ssd, FIONBIO, &u32tmp1);
if(i32tmp1)
{
    printf("Could not set server socket to non-blocking:
%d\r\n", i32tmp1);
}
else

```

```

        {
            printf("Successfully set server socket to non-blocking\r\n");
        }
    }
void set_up_UDP_client(void)
{
    client_length = sizeof(struct sockaddr_in);
    rsd = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
    if (rsd == INVALID_SOCKET)
    {
        fprintf(stderr, "Could not create socket.\n");
        WSACleanup();
        exit(0);
    }
    client_port_number = a4 + PORT_OFFSET;

    rserver.sin_addr.S_un.S_un_b.s_b1 = (unsigned char)a1;
    rserver.sin_addr.S_un.S_un_b.s_b2 = (unsigned char)a2;
    rserver.sin_addr.S_un.S_un_b.s_b3 = (unsigned char)a3;
    rserver.sin_addr.S_un.S_un_b.s_b4 = (unsigned char)a4;
    rserver.sin_port = htons(client_port_number);
    rserver.sin_family = AF_INET;

    sclient.sin_addr.S_un.S_un_b.s_b1 = server.sin_addr.S_un.S_un_b.s_b1;
    sclient.sin_addr.S_un.S_un_b.s_b2 = server.sin_addr.S_un.S_un_b.s_b2;
    sclient.sin_addr.S_un.S_un_b.s_b3 = server.sin_addr.S_un.S_un_b.s_b3;
    sclient.sin_addr.S_un.S_un_b.s_b4 = server.sin_addr.S_un.S_un_b.s_b4;

    sclient.sin_port = htons(client_port_number);
    sclient.sin_family = AF_INET;

    if (bind(rsd, (struct sockaddr *)&sclient, sizeof(struct sockaddr_in))
== -1)
    {
        fprintf(stderr, "Could not bind name to socket.\n");
        closesocket(rsd);
        WSACleanup();
        exit(0);
    }
    else
    {
        printf("Sending Client Socket bound!\r\n");
    }

    i32tmp2 = sizeof(i32tmp1);

    if (getsockopt(rsd, SOL_SOCKET, SO_SNDBUFSIZE, (char*)&i32tmp1, &i32tmp2)
!= SOCKET_ERROR) {
        printf("Receive Time Value: %ld\n", i32tmp1);
    }
    i32tmp1 = RX_BLOCK_TIME;

    if (setsockopt(rsd, SOL_SOCKET, SO_RCVBUFSIZE, (char*)&i32tmp1, i32tmp2)
!= SOCKET_ERROR) {
        printf("Set Receive Time Value: %ld\n", i32tmp1);
    }
}

```

```

        if (getsockopt(rsd, SOL_SOCKET, SO_SNDTIMEO, (char*)&i32tmp1, &i32tmp2)
!= SOCKET_ERROR) {
            printf("Checked Receive Time Value: %ld\n", i32tmp1);
        }
        if (getsockopt(rsd, SOL_SOCKET, SO_MAX_MSG_SIZE, (char*)&i32tmp1,
&i32tmp2) != SOCKET_ERROR) {
            printf("Max Message Length: %ld\n", i32tmp1);
        }
        u32tmp1 = TRUE;
        i32tmp1 = ioctlsocket(rsd, FIONBIO, &u32tmp1);
        if(i32tmp1)
        {
            printf("Could not set client socket to non-blocking:
%d\r\n",i32tmp1);
        }
        else
        {
            printf("Successfully set client socket to non-blocking\r\n");
        }
    }

void set_up_serial_port(void)
{
    //start by making the port name string
    strcpy(port_num, PORTNUMSTR);
    sprintf(portstring, "COM%d", COMport);
    strcat(port_num, portstring);
    //Open up a handle to the serial port
    SPhandle = CreateFile((LPCWSTR)port_num, GENERIC_READ | GENERIC_WRITE,
0, NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
    // Make sure port was opened
    if (SPhandle == INVALID_HANDLE_VALUE)
    {
        printf("Error opening port %i: %s \r\n",COMport, port_num);
//
        exit(0);
    }
    else
    {
        printf("Opened port %i\r\n", COMport);
        printf("GPS Baud Rate needs to be set to 38400!\r\n");
    }
    // Get the port properties
    SPprop.DCBlength = sizeof(SPprop);        /* sizeof(DCB)
*/
    GetCommState(SPhandle, &SPprop);

    SPprop.BaudRate = 38400;        /* Baudrate at which running */
    SPprop.fBinary = TRUE;        /* Binary Mode (skip EOF check) */
    SPprop.fParity = FALSE;        /* Enable parity checking */
    SPprop.fOutxCtsFlow = FALSE; /* CTS handshaking on output */
    SPprop.fOutxDsrFlow = FALSE; /* DSR handshaking on output */
    SPprop.fDtrControl = FALSE; /* DTR Flow control */
    SPprop.fDsrSensitivity = FALSE; /* DSR Sensitivity */
    SPprop.fTXContinueOnXoff = TRUE; /* Continue TX when Xoff sent */
    SPprop.fOutX = FALSE;        /* Enable output X-ON/X-OFF */
    SPprop.fInX = FALSE;        /* Enable input X-ON/X-OFF */
    SPprop.fErrorChar = FALSE; /* Enable Err Replacement */

```

```

SPprop.fNull = FALSE;          /* Enable Null stripping          */
SPprop.fRtsControl = FALSE;   /* Rts Flow control          */
SPprop.fAbortOnError = FALSE; /* Abort all reads and writes on Error */
SPprop.XonLim = FALSE;        /* Transmit X-ON threshold   */
SPprop.XoffLim = FALSE;       /* Transmit X-OFF threshold  */
SPprop.ByteSize = 8;          /* Number of bits/byte, 4-8  */
SPprop.Parity = 0;            /* 0-4=None,Odd,Even,Mark,Space */
SPprop.StopBits = 0;          /* 0,1,2 = 1, 1.5, 2        */
SPprop.XonChar = FALSE;       /* Tx and Rx X-ON character  */
SPprop.XoffChar = FALSE;;     /* Tx and Rx X-OFF character */
SPprop.ErrorChar = FALSE;;    /* Error replacement char    */
SPprop.EofChar = FALSE;;     /* End of Input character    */
SPprop.EvtChar = FALSE;;     /* Received Event character   */

    // Set the port properties
    if (!SetCommState(SPhandle, &SPprop))
    {
        printf("Could not configure serial port\n");
    }
    else
    {
        printf("Serial Port Configured\r\n");
    }
    SetLastError(0);
    if(!GetCommTimeouts (SPhandle, (LPCOMMTIMEOUTS) &SPTimeouts))
    {
        Error = GetLastError();
        printf("Could not get timeouts\r\n");
        printf("Error is %d\r\n",Error);
    }

    // Set the port timeout values
    SPTimeouts.ReadIntervalTimeout=MAXDWORD;
    SPTimeouts.ReadTotalTimeoutConstant=0;
    SPTimeouts.ReadTotalTimeoutMultiplier=0;
    SPTimeouts.WriteTotalTimeoutMultiplier = 0;
    SPTimeouts.WriteTotalTimeoutConstant = 0;

    if (!SetCommTimeouts (SPhandle, (LPCOMMTIMEOUTS) &SPTimeouts))
    {
        Error = GetLastError();
        printf("Could not set timeouts\r\n");
        printf("Error is %d\r\n",Error);
    }
    else
    {
        printf("Serial Port Timeouts Set\r\n");
    }
}

```

APPENDIX C: PLOTS OF INDIVIDUAL RUNS

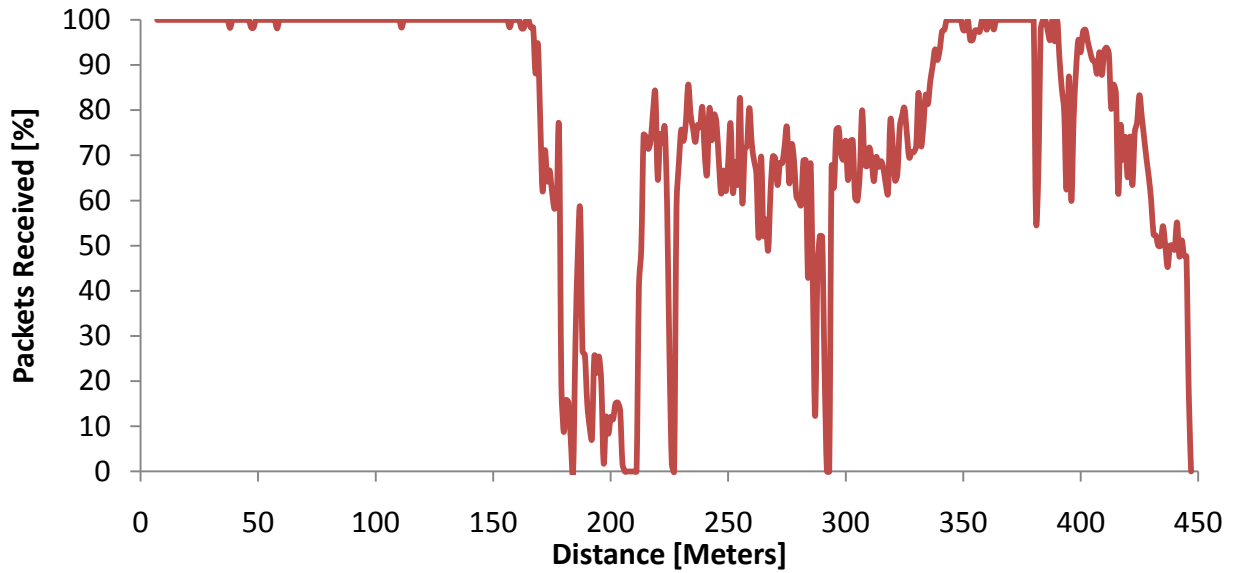


Figure 40. Plot of packets received versus distance using 802.11b at 1 Mbit/sec and antenna height of 3.47 meters (Run 1).

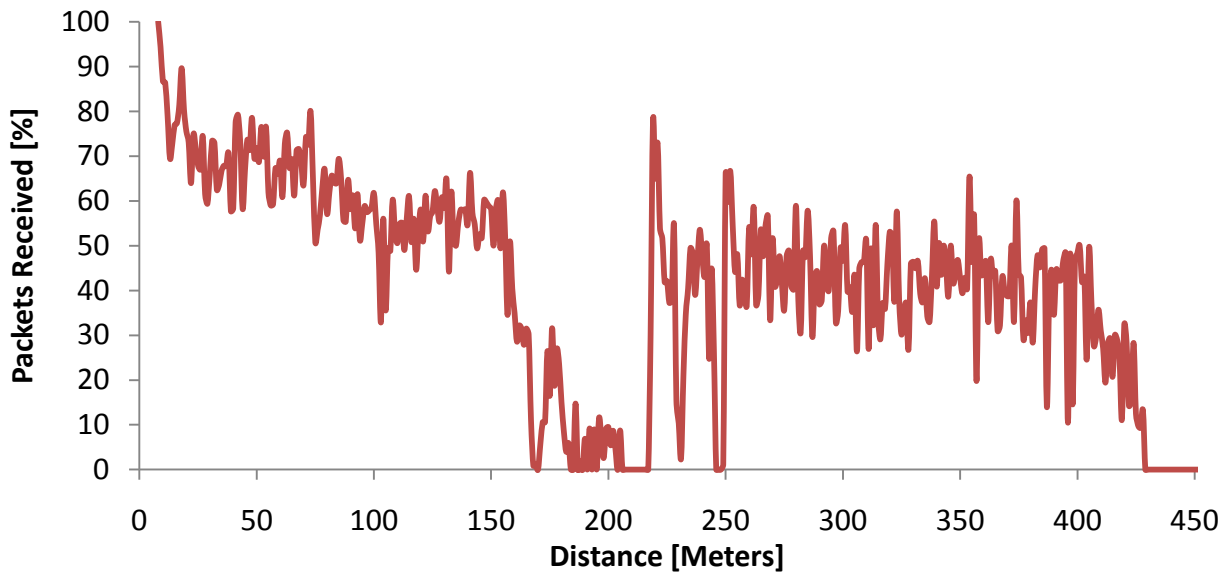


Figure 41. Plot of packets received versus distance using 802.11b at 2 Mbits/sec and antenna height of 3.47 meters (Run 2).

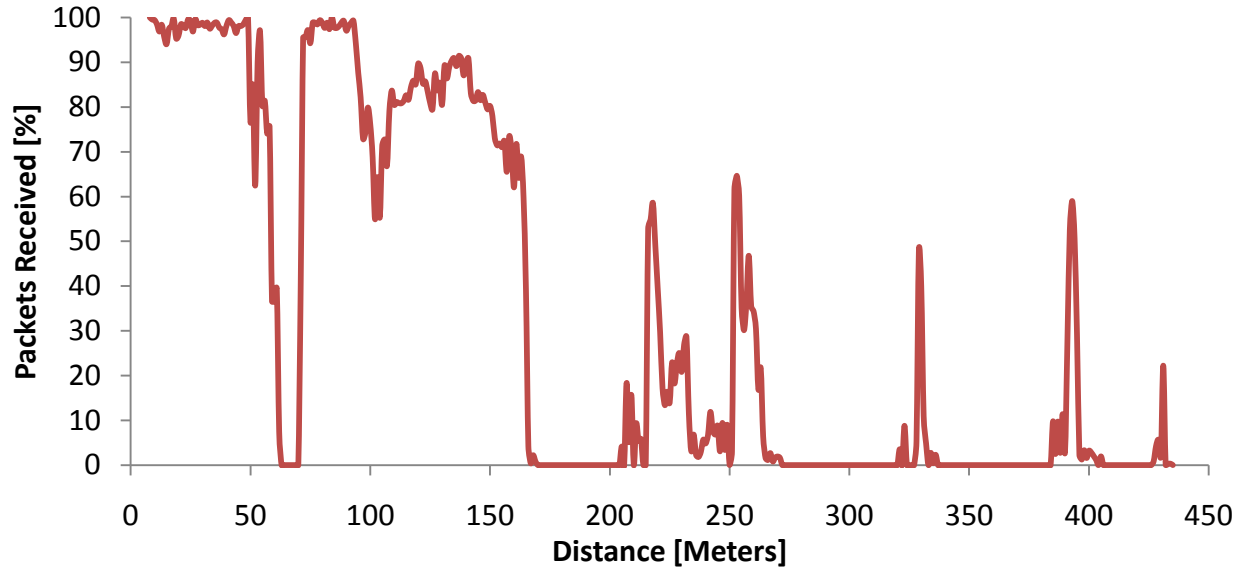


Figure 42. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 3).

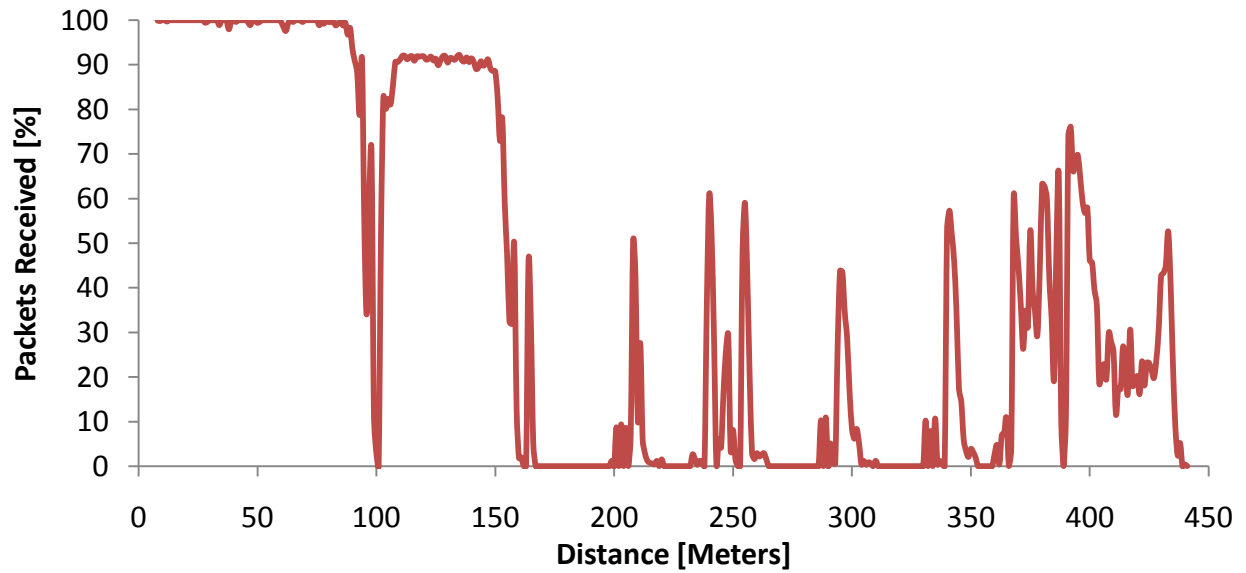


Figure 43. Plot of packets received versus distance using 802.11g at 12 Mbits/sec and antenna height of 3.47 meters (Run 4).

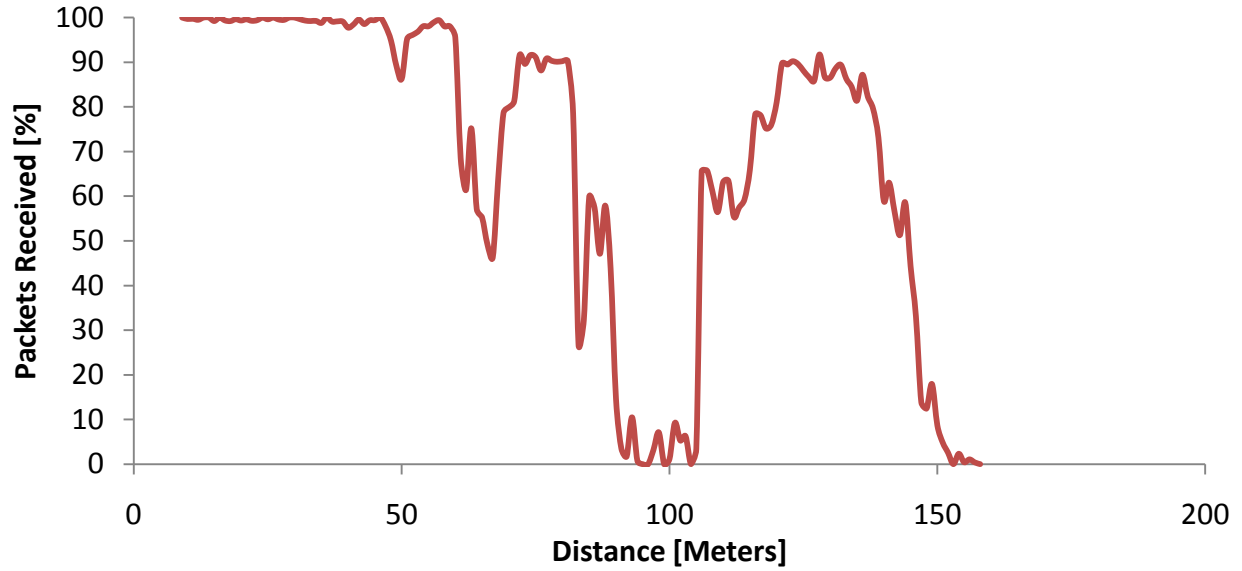


Figure 44. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 5).

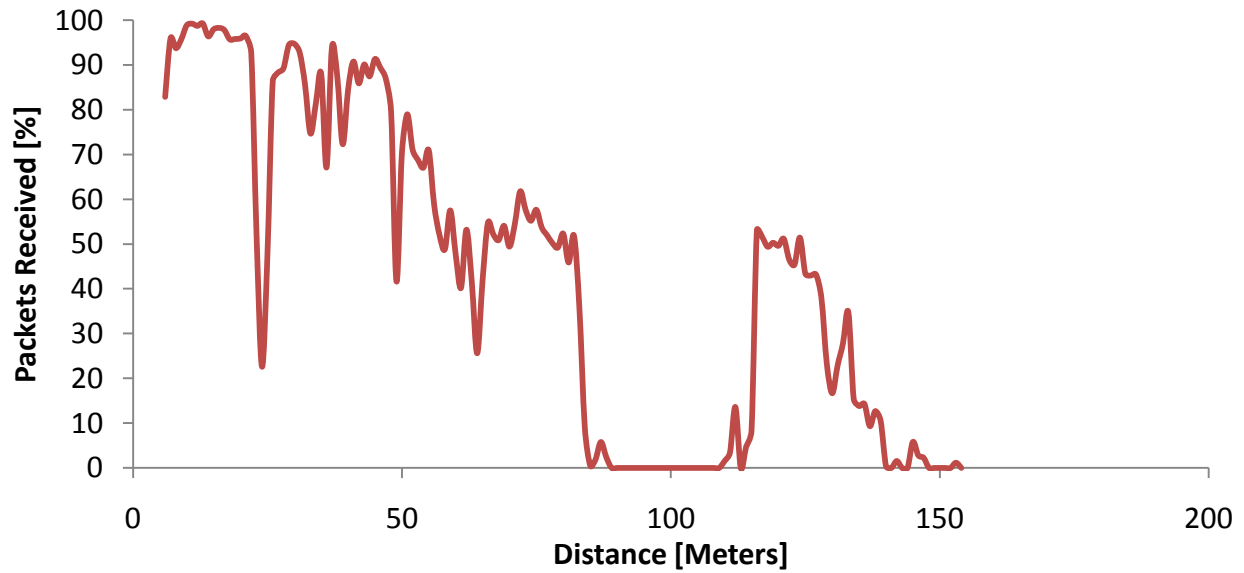


Figure 45. Plot of packets received versus distance using 802.11g at 36 Mbits/sec and antenna height of 3.47 meters (Run 6).

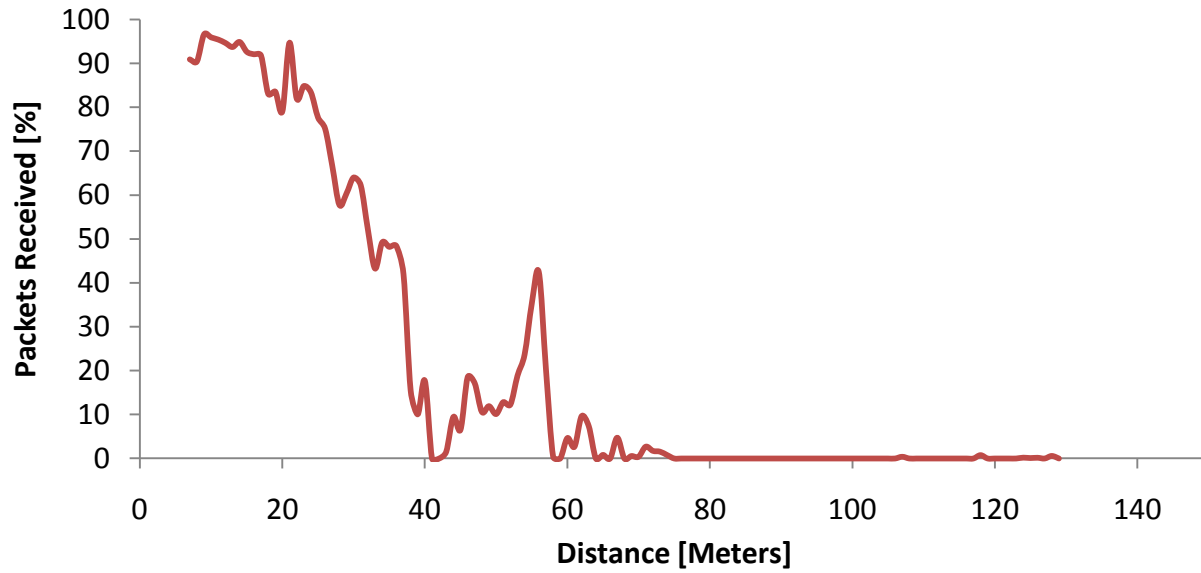


Figure 46. Plot of packets received versus distance using 802.11g at 54 Mbits/sec and antenna height of 3.47 meters (Run 7).

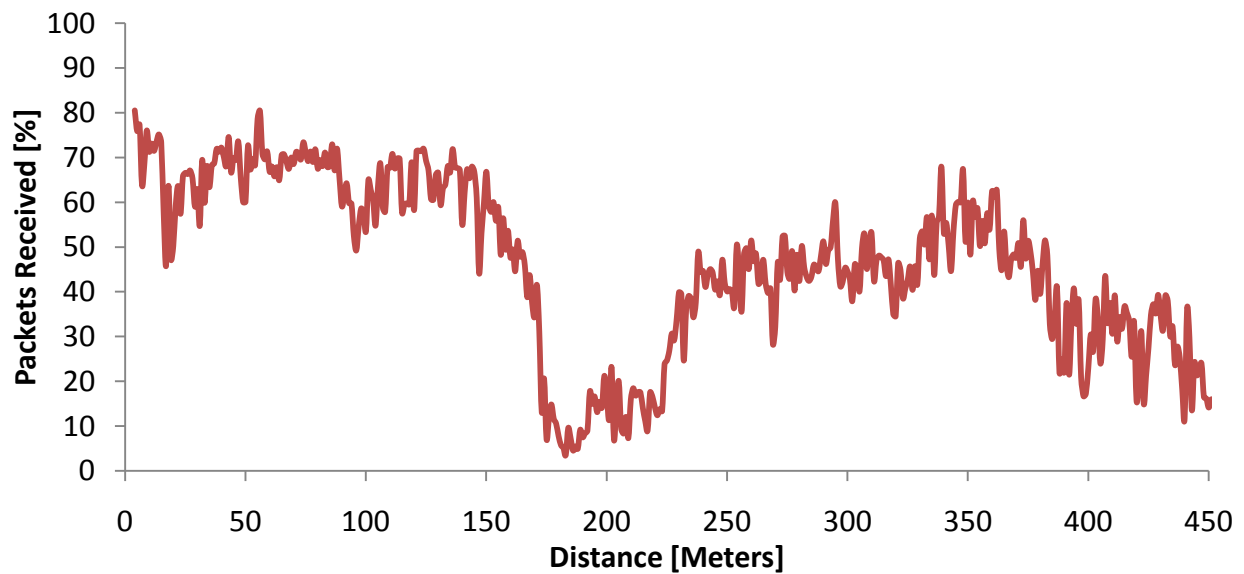


Figure 47. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 8).

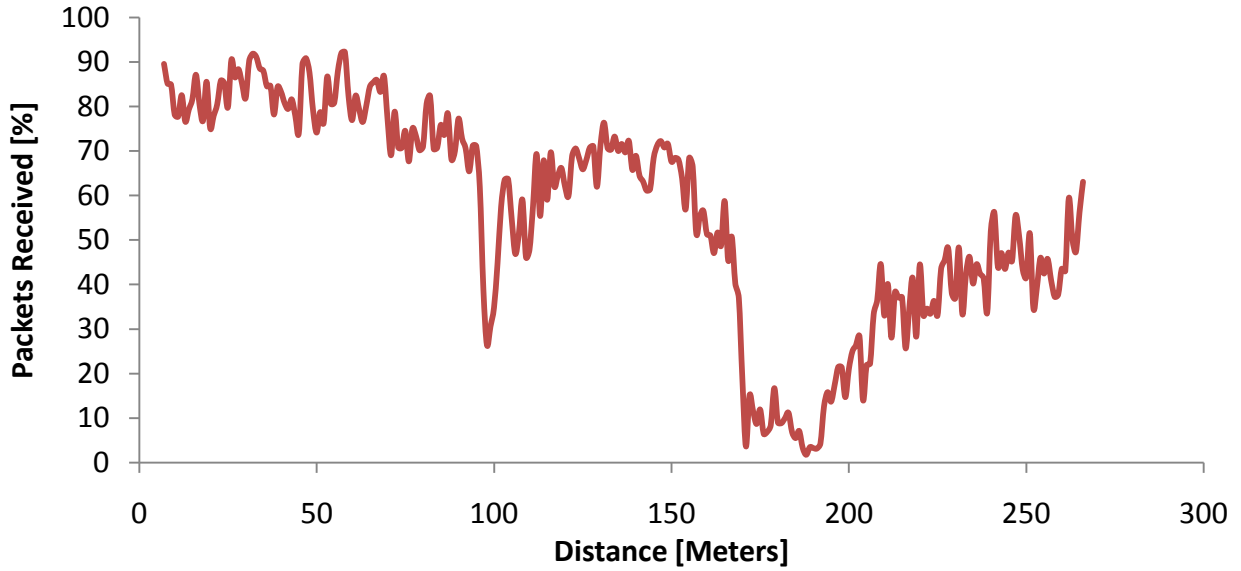


Figure 48. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 9). Tractors drove back to starting position in reverse.

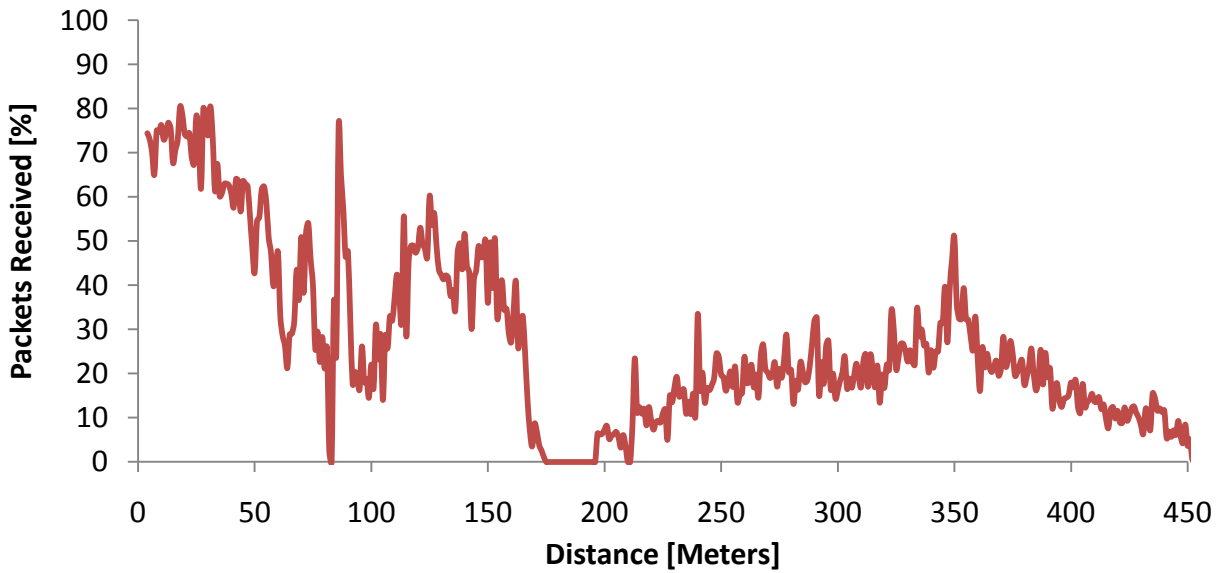


Figure 49. Plot of packets received versus distance using 802.11b at 5.5 Mbits/sec and antenna height of 3.47 meters (Run 10).

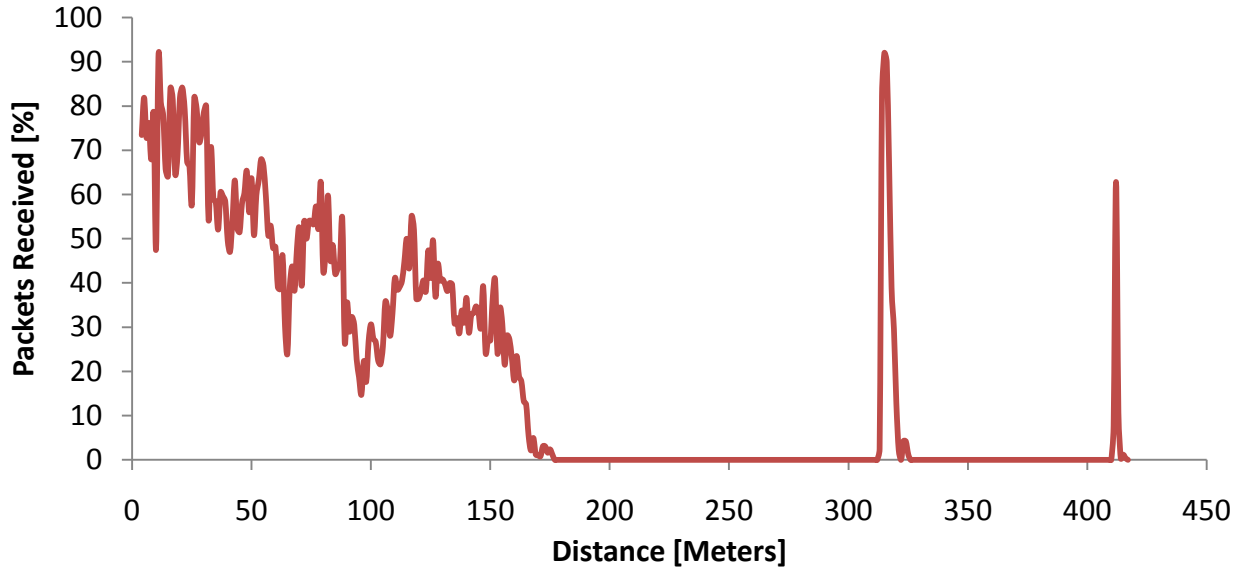


Figure 50. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 11).

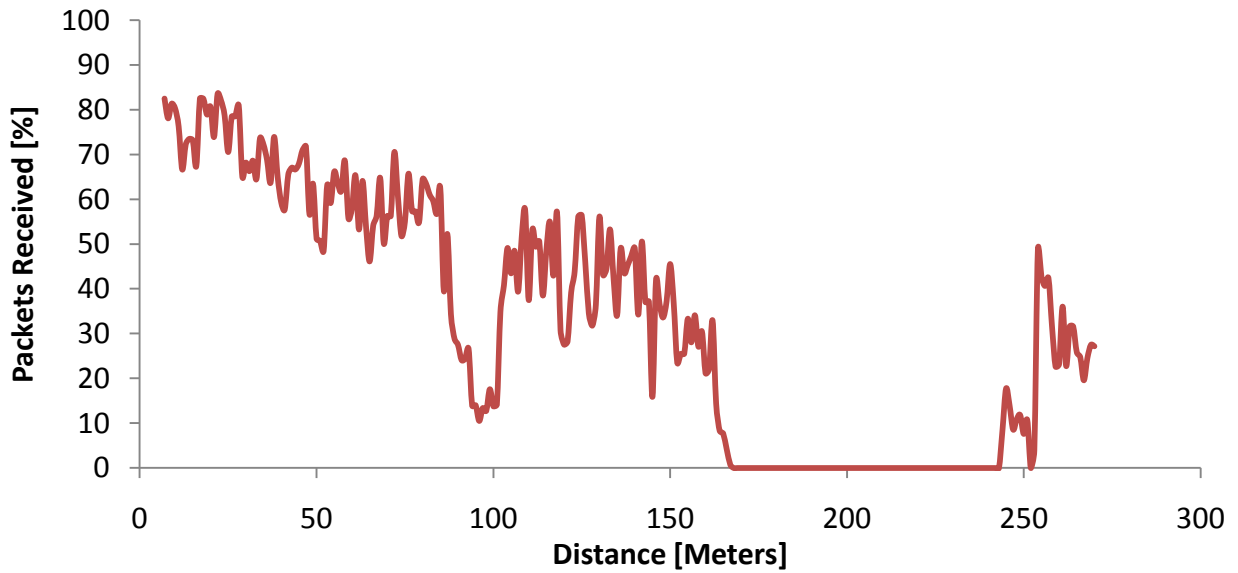


Figure 51. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 3.47 meters (Run 12). Tractors drove back to starting position in reverse.

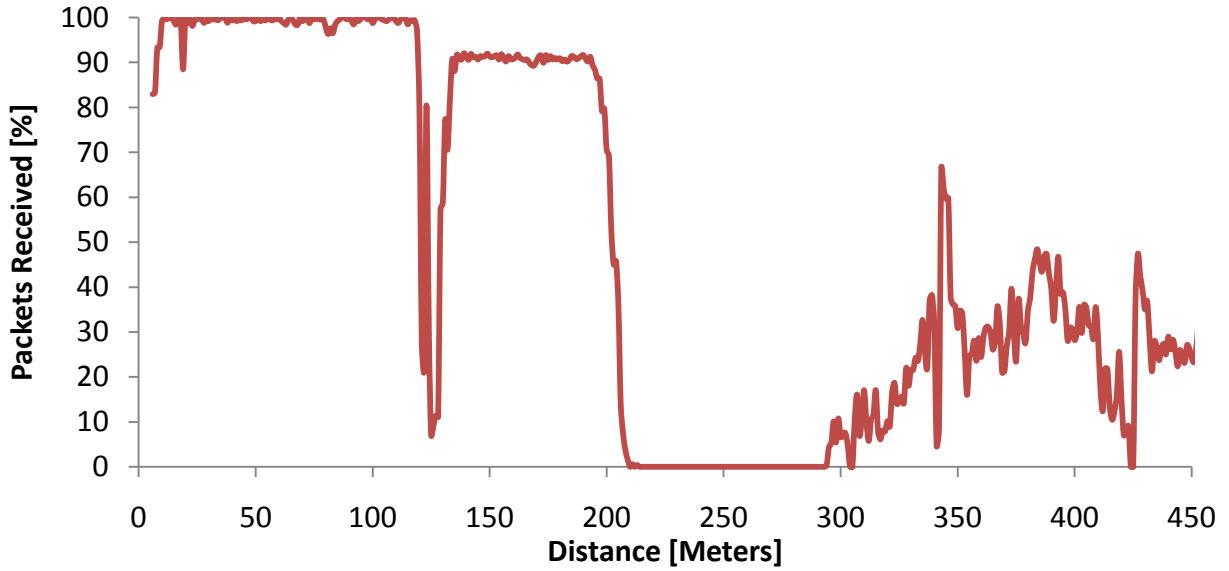


Figure 52. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 13).

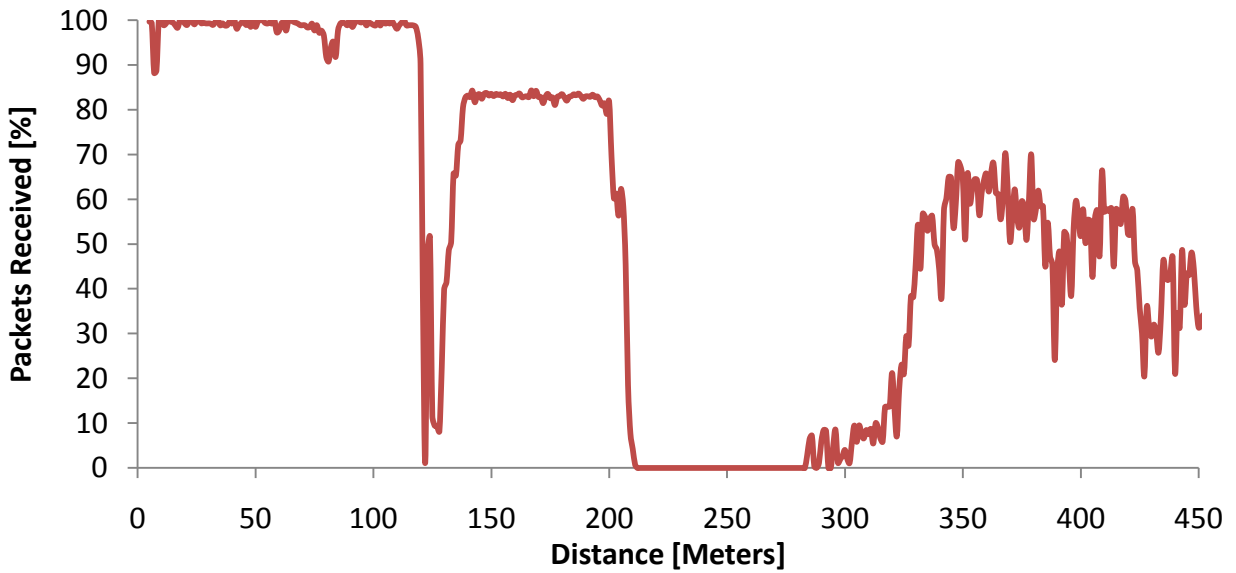


Figure 53. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 4.00 meters (Run 14). Tractors drove back to starting position in reverse.

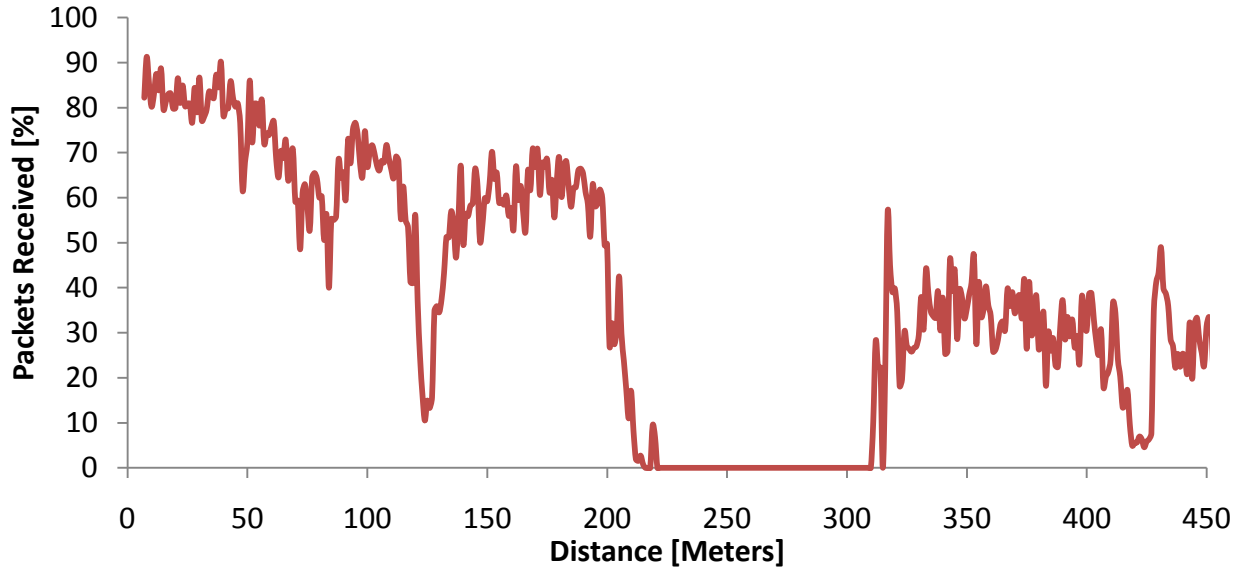


Figure 54. Plot of packets received versus distance using 802.11g at 6 Mbits/sec and antenna height of 4.00 meters (Run 15). Tractors drove back to starting position in reverse.

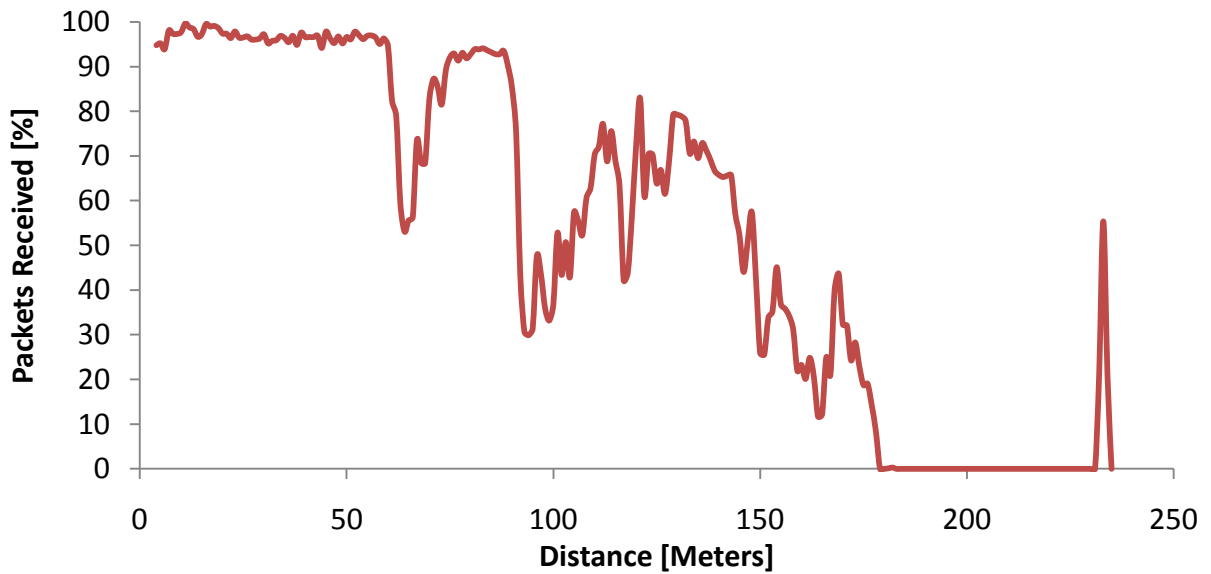


Figure 55. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 16).

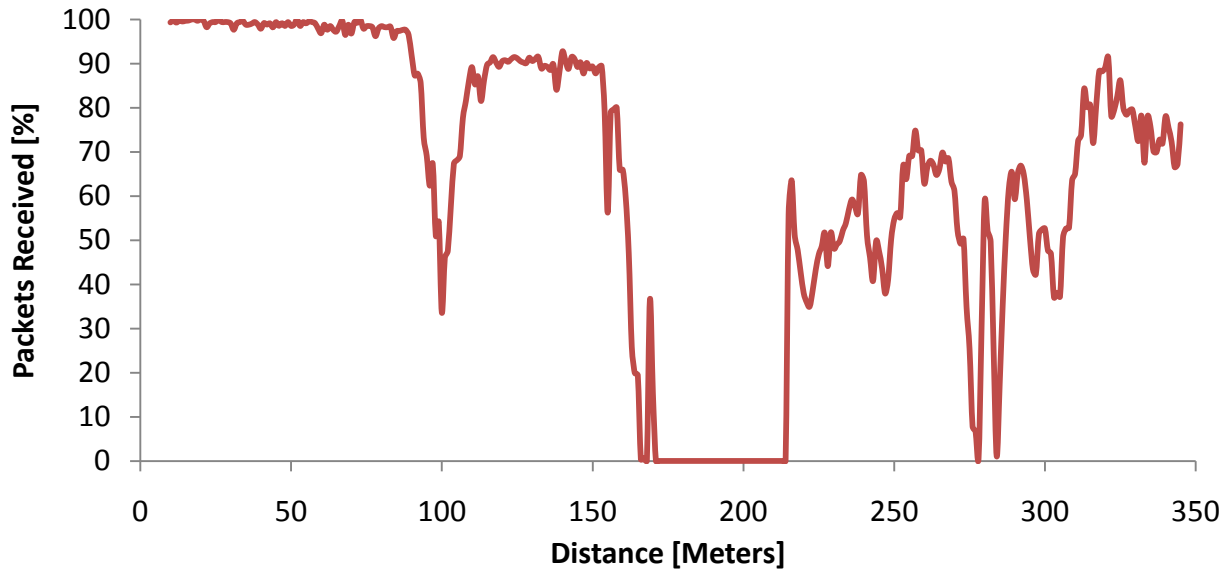


Figure 56. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 17). One vehicle remained stationary while the second drove pattern A.

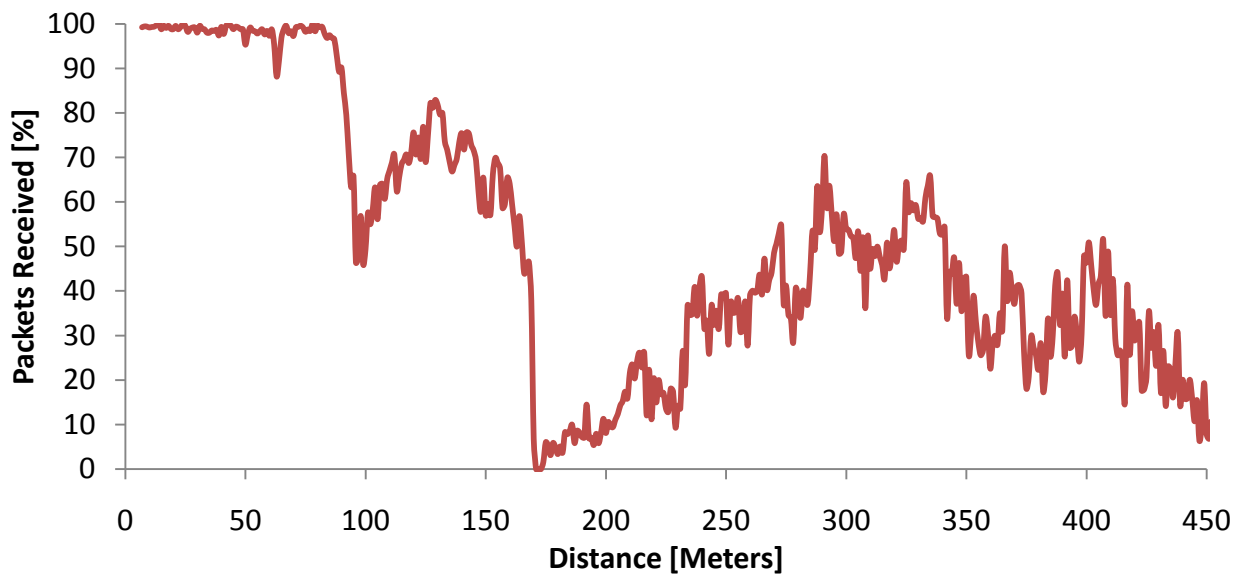


Figure 57. Plot of packets received versus distance using 802.11g at 18 Mbits/sec and antenna height of 3.47 meters (Run 18). Radio configurations were swapped for this run.