NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WIRELESS SENSOR NODE DATA GATHERING AND LOCATION MAPPING

by

Todd E. Sims

March 2012

Thesis Advisor:	Weilian Su
Second Reader:	Xiaoping Yun

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** MARCH 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE Wireless Sensor Node Data Gathering and Location Mapping		**5. FUNDING NUMBERS**
6. AUTHOR(S) LT Todd E Sims		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. I.R.B. Protocol number NA.		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

With advances in wireless communications and miniaturization of mobile sensors, Wireless Sensor Nodes are increasingly being deployed in Ad Hoc fashions. Efficiently gathering data from the networks now becomes a larger problem. Collecting sensor data from a group of nodes deployed in an unknown arrangement in the shortest amount of time requires the collector to utilize a methodology that minimizes collection overlap. Inexpensive commercial off-the-shelf wireless routers and mobile platforms that can be utilized to fly over a field of wireless nodes and create a link connecting to and retrieving the maximum amount of data, are examined in this thesis. The problems are two-fold: first, the necessary task of locating the wireless devices in a given area, querying these devices to collect raw data for positioning, and second, the task of then creating a static map of derived locations.

In order to enumerate device locations, the relationship of signal strength measurements and round trip signal times between wireless nodes and the wireless access router were investigated in this thesis. The results of this research support the conclusion that an inexpensive collection system can be readily configured for the task of automated client surveying and distance approximation.

14. SUBJECT TERMS IEEE 80211 Standards, Wireless sensor networks, Mobile ad hoc networks			**15. NUMBER OF PAGES** 53
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WIRELESS SENSOR NODE DATA GATHERING AND LOCATION MAPPING

Todd E. Sims
Lieutenant, United States Navy
B.S., Hawaii Pacific University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
MARCH 2012

Author: Todd E. Sims

Approved by: Weilian Su
Thesis Advisor

Xiaoping Yun
Second Reader

R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

With advances in wireless communications and miniaturization of mobile sensors, Wireless Sensor Nodes are increasingly being deployed in Ad Hoc fashions. Efficiently gathering data from the networks now becomes a larger problem. Collecting sensor data from a group of nodes deployed in an unknown arrangement in the shortest amount of time requires the collector to utilize a methodology that minimizes collection overlap. Inexpensive commercial off-the-shelf wireless routers and mobile platforms that can be utilized to fly over a field of wireless nodes and create a link connecting to and retrieving the maximum amount of data, are examined in this thesis. The problems are two-fold: first, the necessary task of locating the wireless devices in a given area, querying these devices to collect raw data for positioning, and second, the task of then creating a static map of derived locations.

In order to enumerate device locations, the relationship of signal strength measurements and round trip signal times between wireless nodes and the wireless access router were investigated in this thesis. The results of this research support the conclusion that an inexpensive collection system can be readily configured for the task of automated client surveying and distance approximation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

With advances in wireless communications and miniaturization of mobile sensors, Wireless Sensor Nodes are increasingly being deployed in Ad Hoc fashions. Efficiently gathering data from the networks now becomes a larger problem. A method to quickly enumerate wireless nodes automatically, gather location information and collect data in a given area that will enable post survey registering to collected Global Positioning System (GPS) coordinates would be beneficial to anyone tasked with surveying and retrieving the data stored in the field of wireless devices. Inexpensive commercial-off-the-shelf wireless routers and mobile platforms that can be utilized to fly over a field of wireless nodes and create a link connecting to and retrieving the maximum amount of data were examined in this thesis. The problems are two-fold: first, the necessary task of locating the wireless devices in a given area, querying these devices to collect raw data for positioning, and second, the task of then creating a static map of derived locations.

The use of the Internet Control Message Protocol (ICMP) echo message packets to calculate distance from time-of-arrival (TOA) measurements was examined. This method was deemed inappropriate due to lack of sufficiently precise timestamps in the IEEE 802.11g protocol implementation. Range-based measurements from the commercial-off-the-shelf components (COTS) access point employed were found to be a highly reliable means to calculate distance in the outdoor environment when used with a specifically calibrated range table. Further work was done to craft a low cost COTS implementation of a wireless node survey tool from common components. This device proved to be small, robust and independently capable of surveying a gridded test map of wireless nodes. The measurements gathered from the field surveys were sufficiently accurate enough to provide location fix data for a sensor node with 85% accuracy pinned to a 10 foot square grid. Follow-on work to affix this system to an airborne collection platform, possibly providing autonomous flight guidance based upon sensor surveying, is recommended.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AOR	Angle of Arrival
AP	Access Point
BS	Base Station
COTS	Commercial Off-the-Shelf
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
JTAG	Joint Test Action Group
RC	Radio Controlled
RDOA	Range Difference of Arrival
RF	Radio frequency
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
SNR	Signal-to-noise ratio
TTL	Transistor-transistor logic
WAP	Wireless Access Point
Wi-Fi	Wireless Fidelity (IEEE 802.11g)
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Networks

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife, Jane, my son, Zachary, and my daughter, Piper, for their patience and steadfast devotion. Without them, this thesis would have not been possible.

Dr. Su, your direction and support were invaluable.

To all NPS professors and staff, who imparted the knowledge and years of wisdom to help me accomplish this thesis, thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The increased miniaturization and processing power of integrated circuits has made for the ability to have extremely capable networking gear available in very small packages. We now can provide robust Wireless Fidelity (Wi-Fi) routing anywhere deemed necessary for very little cost. We now have wireless networks everywhere imaginable, in the car, fast food restaurants, libraries and many public places. The United States Military has leveraged these technologies for use in the battlefield, researching and deploying mobile ad hoc sensor networks. Ad hoc sensor networks can communicate point-to-point to other radio nodes within range and also communicate with wireless access points to route traffic back when available. Mobile ad hoc nodes can be deployed with these gateway access points that relay data to another network, typically using another communications protocol. These gateway access points, however, need to be placed strategically and operate automatically in an unknown environment so they can communicate with the largest number of nodes yet still be able to communicate back to the gateway network. As a result of miniaturization, we are able to attach a commercial off-the-shelf wireless router to an aerial platform to provide a convenient communication relay back to the user. The mobile router, however, needs to be placed in an optimal location in order to provide the best coverage of the sensor network. The first step in efficient placement is node localization. The recent proliferation of inexpensive wireless access points with signal strength and propagation time recording capabilities allows for the convergence on a small platform, a device that can simultaneously provide backhaul communications for a network of wireless nodes and also provide enough detailed information to locate these devices.

Recently some work has done to overcome the problems of accurate Wi-Fi signal emitter location. Some intriguing solutions have been proposed. Wenyao Ho et al. [1] presented a solution with a two-phase approach. First, they used a traditional radio frequency (RF) energy pattern matching to identify a general location of a given signal. Then, by utilizing pre-trained maps, localization was iteratively resolved finer with each

subsequent test run. Finally, they used logistic regression to determine the most likely relationship between path loss and distance. The second insightful phase to their research was in applying the pre-trained maps and distance estimations in real time to obtain estimations that were 95% accurate in observed tests.

Wang, Gao, and Wang [2] investigated methods for increased accuracy of user location when using Wi-Fi by utilizing a new algorithm for calculating the Received Signal Strength (RSS) to position mobile terminals. In addition to calculating the distance by using RF signal measurements and time averaging, an interesting approach to eliminate signal fluctuations was to use time-based pattern matching as reported by [3]. By watching the signal for an extended duration, they were able to show that, although the signal strength of a given emitter varies randomly, with time a real-time location sensor could be developed. Although both implantations yielded good results, they required custom hardware and software to realize their solutions. There are some lessons to be learned through these approaches. Utilizing pre-trained calibration maps and collecting data in statistically large amounts, we hope that source localization can be accomplished with off-the-shelf components. Mohit Soxena, Puneet Gupta and Bijendra Jain [4] investigated a similar method of calibrating RSSI values prior to calculating distance measurements. In this thesis, we investigate a best-case scenario where the effects of Rayleigh fading are minimized by running tests in an outdoor range. By designing a system within the limitations of inexpensive COTS hardware, the limitations and feasibility of the proposed methods are investigated.

B. PURPOSE

Currently, the methods for enumerating locations of wireless devices involve adding GPS modules to each device or having prior knowledge of fixed access point locations in order to build location maps. The viability of using inexpensive wireless routers in order to gather data and location information is examined in this thesis. Additionally, the possibility of mounting the necessary hardware on a hobby radio control (RC) platform and still having flight times long enough to query and retrieve data from a field of wireless devices is also examined.

C. RESEARCH QUESTIONS

This thesis is focused on answering three basic questions related to inexpensive Wi-Fi client enumeration. Is there a method to calculate the location of unknown wireless emitters outdoors utilizing only an inexpensive Wi-Fi router? Can such an implementation be combined with a small aerial platform to collect and map such data? And, finally, could such a system provide geolocation data with enough resolution to provide for automated sensor surveying and mapping?

D. THESIS ORGANIZATION

The organization of the thesis is as follows. The wireless device technologies and methods that can be employed for enumeration and localization are introduced in Chapter II. The modifications of the Linksys WRT-54GL wireless router and the test-bed setup are covered in Chapter III. The data collected is examined and analyzed in Chapter IV. The conclusion and future research topics are given in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS DEVICE ENUMERATION

A. LOCALIZATION OF WIRELESS SIGNALS

The specific location of an unknown signal can be calculated with two distinct methods. Triangulation is the use of geometric angle measurements to a signal source from two or more known points. More pertinent to this work is trilateration, which uses distance measurements gleaned from signal strength measurements or round trip time of flight measurements. There have been studies that have examined wireless positioning techniques using time-of-arrival (TOA) based location systems such as closest neighbor or other weighting methods [5]. However, specific laboratory gear must be utilized in order to capture high resolution data in all of the previous approaches examined.

B. IEEE 802.11 RANGE AND CHANNELS

The most common form of IEEE 802.11 wireless local area network (WLAN) standards in use at the time of this writing is IEEE 802.11g, known commercially as Wi-Fi. This third generation of the WLAN standard uses the 2.4 GHz band and operates at a maximum raw data rate of 54 Mbps. This robust standard allows for multiple channel assignments and various data rates and is backward compatible with older standards, which has allowed the technology to proliferate in low cost implementations. The ubiquity of wireless access points and sensor nodes that also utilize IEEE 802.11g allows for seamless interoperability between many commercial-off-the-shelf components. Typical peak power output of these devices is 100 mW with ranges outdoors at up to 300 ft. The IEEE 802.11g employs orthogonal frequency-division multiplexing (OFDM) for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Graceful degradation allows for step back to lower data rates as signal-to-noise ratio (SNR) is affected by noise in the environment or as distances between nodes increase. The modulation and data rates for this standard are summarized in Table 1.

Table 1. Coding and modulation in IEEE 802.11 standard (From [6]).

Data rates (Mbps)	Modulation type	Error correction
6	BPSK	1/2
9	BPSK	3/4
12	QPSK	1/2
18	QPSK	3/4
24	16-QAM	1/2
36	16-QAM	3/4
48	64-QAM	2/3
54	64-QAM	3/4

C. RSSI MEASURING AND DISTANCE APPROXIMATION

Received signal strength indicator (RSSI) is defined by the IEEE as a mechanism by which RF energy is to be measured by the circuitry of the wireless Network Interface Card (NIC). In practice, manufacturers have implemented these measurements in various ways. In the Linksys wireless access point utilized in this thesis, the measurements are abstracted from the onboard analog-to-digital converter (ADC) and reported as dBm. The overall goal of gathering RSSI values is to characterize the relationship between RSSI readings and distance approximations. The reduction in received signal power over a given distance is given by [7]:

$$L_{pathloss} = \frac{P_r}{P_t} = G_t G_r \left[\frac{\lambda}{4\pi d}\right]^2 \quad (1)$$

where $L_{pathloss}$ is the path loss at distance d, calculated as a ratio between the transmit power P_r and the receiver power P_t. The power gain of each antenna is similarly represented as G_t and G_r, respectively. The wavelength is represented as λ. In order to

facilitate quick calculations in the field we substitute the static values for the transmit power, receive antenna gain, transmit antenna gain, and wavelength λ at 75.0 mW, 7.0 dB, 7.0 dB and 2.432 GHz, respectively. Therefore, the free space path loss is now given by:

$$L_{pathloss} = 40.23 + 20\log(d). \quad (2)$$

This approach simplifies the path loss calculation, disregarding fading from multipath and other sources; these calculations will offer a baseline to compare against empirical results. The next step is to calibrate the observed RSSI values at pre-determined distance intervals and use actual data to generate x, y pairs for location prediction. RSSI measurements conducted indoors correlate poorly with actual observed distance as seen in [8] due to attenuation, reflection and scattering, but in this thesis RSSI in an outdoor rural environment is considered. A method of statistical averaging and calibration mapping against premeasured values is examined to provide sufficient resolution for unambiguous location data.

D. ROUND-TRIP TIME

Initially, the feasibility of utilizing the time-of-flight measurements of an Echo packet to calculate distance from node to router was examined. The internet control message protocol (ICMP) ping packet round-trip time (RTT) response was examined due to the timestamp calculations inherent in the protocol. Ping was created early on in the development of IP networks and is appropriately named for its ability to acknowledge if a distant node is responding in an appropriate time. Round-trip time from a wireless access point to the attached client includes the time it takes for the physical signal to travel to the device, the client card processing time plus the length of time to receive the acknowledgment. Although this approach seemed uniquely suited to provide response time for detailed distance calculations, this approach was eventually abandoned due the lack of high resolution timestamp reporting in the standard IEEE 802.11 protocol. However, it was discovered that there has been some work in using custom hardware to

gather high precision timing from the physical layer of the wireless interface [9]. This approach was deemed outside the scope of this thesis in that the proposed thesis solution is primarily using COTS hardware to determine device location.

III. EXPERIMENTAL SETUP

A. LINKSYS WRT-54GL MODIFICATIONS

The Wireless Access Point (AP) that was selected for this thesis was the Linksys WRT54GL AP (Figure 1), which utilizes a well-understood but underutilized Broadcom BCM2050 radio chipset. This BCM2050 chipset was focused on in this research due to its ubiquity in consumer grade networking gear and that it also can also be modified to run a light version of a Linux based operating system. With some minor hardware and software modifications, the Linksys WRT-54GL is tailored to become a suitable platform for this research. The Linksys WRT-54GL is capable of acting as a standard WAP for relaying of wireless sensor data while simultaneously collecting and storing data. By examining the WRT-54GL in detail and changing the generic operating firmware, we configured the Wi-Fi router to accept serial communications, USB connectivity, Joint Test Action Group (JTAG) programming, GPS reporting and a secure digital (SD) media card for onboard storage. The WRT-54GL has a main CPU that runs at 200 MHz, 16 MB of flash ram and 4 MB of ROM, which was utilized to enable the device to perform the functions of a fully-fledged computer. Detailed in the following steps are the particular modifications that were made to enable this device to collect the necessary data.

Figure 1. Linksys WRT-54GL wireless router.

B. DD-WRT FIRMWARE

The Broadcom BCM2050 radio chipset is ubiquitous in wireless access points manufactured by Linksys and other manufacturers, which has had a robust following by open source software (OSS) developers. By installing OSS firmware that replaces the default installation, many hidden features were enabled. The process for installing a custom operating system is easy and straightforward through the standard web interface that ships with all Linksys devices. There are many third party firmware loads available for Linksys routers and access points. The OSS firmware, DD-WRT, was chosen for ease of use and the ability to control many actions via scriptable commands. For this thesis DD-WRT version 2.4 is used [10].

C. SERIAL PORT ACCESS

The Linksys WRT-54GL has most of the circuitry on the main board for serial communications. Some minor modifications are necessary to enable serial port use in this experiment. The hardware configurations are depicted in Figures 2 and 3. The first step in order to utilize the serial ports is accomplished by updating the software to DD-WRT. The second step is to add a small amount of hardware in order to make the necessary voltage level transitions for greater compatibility with different external devices. The WRT-54GL main board has an unpopulated area that can be used along with a transistor-transistor logic (TTL) to serial translator chip to accommodate for voltage and timing differences between the WRT-54GL and standard computer serial ports. In this research, the MAX232 chip from Maxim was chosen due to the price and since it was available as a discrete through-pin component, greatly simplifying the steps necessary to expand the system for this capability.

Figure 2. MAX232 and components (From [11]).

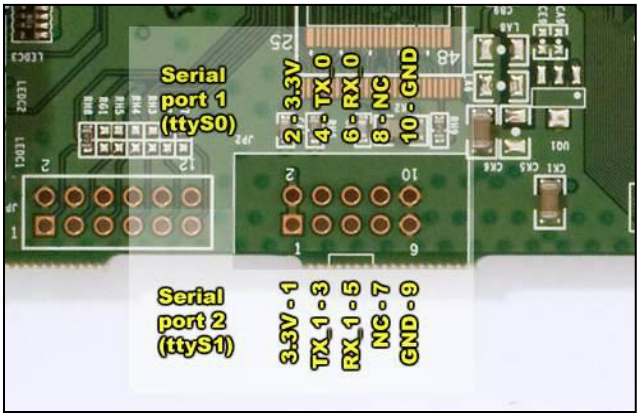

Figure 3. MAX232 pin outs (From [11]).

Once the MAX232 DIP chip is connected to the main board's power and to the TTL receive and transmit pins, the ability for the wireless access point to communicate to serial devices can be enabled through the advanced configuration web page, which is accessible at the local host address of 192.168.1.1. Alternatively, this can also be accomplished by sending the serial commands listed in Figure 4; the commands are entered from a shell interface. Through this method, we can access the settings, such as communication speed. For this thesis, an additional configuration script was downloaded. The script can set the serial port to communicate with external devices at 4,800 baud.

```
#ipkg update
#ipkg install setserial
#wget http://tobe.mine.nu/software/openwrt/stty.tgz
#tar –zxvf sty.tgz
#chmod 755 stty
#setserial /dev/tts/1 irq 3
#setserial /dev/tts/1 raw speed 4800
```

Figure 4. SSH commands to enable serial port.

D. GLOBAL POSITIONING SYSTEM (GPS)

A method to timestamp the collected data and to geo-locate the collection platform was necessary for this experiment. An idea that presented itself after a serial port upgrade on the Linksys WRT-54GL was to add on a GPS unit that could then communicate serially with the Linksys AP. A GPS unit was chosen for the AP to provide initial location registration to differentiate multiple data sets collected in various outdoor locations. This method worked flawlessly throughout the test runs and provided GPS coordinates to the system, which were then used to time and location stamp each subsequent set of data collected. COTS GPS units built for original equipment manufacturers (OEMs) can be purchased for under $50; the units are serial port accessible. EM-406A SIRF III 20 Channel receiver (Figure 5) was selected for its high sensitivity receiver that worked with partial sky view obscuration by the host platform.

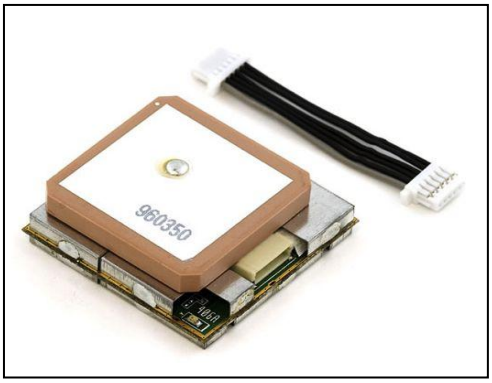

Figure 5. EM-406A OEM GPS unit (From [12]).

E. SECURE DIGITAL CARD LOGGING

Internally, the system does not have a large amount of non-volatile random access memory (NVRAM) necessary for logging and storing of node data. Again, the Linksys WRT-54GL Access Point has unpopulated general purpose input/output (GPIO) ports that can be enabled to work with secure digital (SD) data cards to provide for the requirements of extended data storage and offer the user a quick retrieval method in case of an aerial platform failure. For this modification, a discarded floppy disk ribbon cable was all that was needed to make the connection. This no cost item was and trimmed to match the size of the SD card I/O pins. This cable was soldered directly onto the WRT-54GL main board according to the configuration specified in Table 2.

Table 2. SD card to WRT-54GL connections (From [11]).

SD Card Pin	**WRT54-GL Connection**
1 Chip Select	GPIO 7
2 Data In	GPIO 2
3 VSS -Power	Ground
4 VDD +Power	3.3V
5 Clock	GPIO 3
6 VSS2 Secondary -Power	Ground
7 Data Out	GPIO 4

With the added convenience of having a long ribbon cable, the SD card can be mounted anywhere in the case or on the mobile platform itself. For this experiment, the device was mounted externally for convenience to confirm operability. Afterwards, the SD card was mounted inside the Linksys WRT-54GL casing. To utilize the SD Card under DD-WRT or other OS packages, the steps are the same after physically connecting the pins. From a shell command line, the commands in Figure 6 are entered. The only

limitation to this design was in choosing an SD card that is under 2 GB or less in capacity for compatibility with multiple operating systems.

```
# ipkg update
# ipkg install kmod-vfat
reboot device
# scp \mmc.o>\root@192.168.1.1\lib\modukles\2.4.30\mmc.o
# insmod mmc.o
# dmesg
```

Figure 6. SSH commands to enable SD card use under DD-WRT.

F. POWER

The Linksys WRT-54GL comes with a typical 120 VAC wall mounted switching power supply providing 12 VDC at 1 A. In testing, the power draw was noticeably less than 1 A. A quick search provided an 8 AA cell battery pack that was modified to seamlessly connect to the WRT-54GL power input jack. This provided several advantages: over five hours run time during multiple real-world tests, increased portability, and platform independence with only a very modest increase in overall weight. Other ideas were considered, such as powering the unit directly from the aerial platform batteries or from photo voltaic (PV) cells. The complexity of leeching power from the transport platform limited platform choices, and PV cells proved too cumbersome and complex to include on a moving device.

G. ADDITIONAL MODIFICATIONS

The Linksys WRT-54GL utilizes two omnidirectional rubber-ducky type antennas. The default configuration allows either antenna to automatically switch between transmit or receive dynamically as signal conditions change. In order to minimize antenna diversity issues and to enable measurements that are not angle dependent, the setting is enabled so the right antenna is set to transmit and the left

antenna is set to receive. In practice, this setting was enabled, resulting in ambiguous RSSI measurements. Additionally, the IEEE 802.11g Wi-Fi standard allows for client and access point to negotiate channels dynamically, which would affect RSSI measurements. The access point and clients were locked on a single channel (Channel 5, 2.432 GHz) to lessen the introduction of non-linear errors in RSSI correlation.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERFORMANCE EVALUATION

A. TESTBED SETUP

A test-bed was set up on the Naval Postgraduate School (NPS) baseball field that allowed for testing outdoors away from large building or hard surfaces. Additional wireless network devices were employed to play the role of a wireless node. The tests were broken up into three distinct phases and performed in multiple iterations over several weeks. The first test was performed in order to confirm platform suitability and to build a calibrated map of RSSI measurements observed. The second test phase was a trial run of the scripting that was necessary in order to employ automatic data collection and logging. The final test phase employed all of the lessons learned in the previous steps and utilized the calibrated RSSI readings in order to automatically query and map a group of wireless devices placed in an open field with locations unknown beforehand.

1. TEST PHASE ONE

This test was performed at the NPS baseball field using the newly configured Linksys WRT-54GL containing SD card access, GPS communication ability and onboard power. Communication with the access point was accomplished via an extended Ethernet cable, and the commands were manually entered to confirm efficient methodologies for later use. The wireless AP was tethered to a large pole to simulate an aerial collection system and measurements were taken in 10 ft increments away from distant node. The location markers from start to finish are displayed in Figure 7. In the experimental trials, noticeable changes in values did not occur with step sizes below 10 ft. For initial characterization, measurements were performed in 10 ft increments in ranges from 0 to 200 ft. The RSSI values were observed and averaged over 30 second increments from the distant node. The calculated mean values are displayed in Table 3.

Figure 7. Test 1 test pattern (From Google Earth).

Table 1. Average RSSI measurements.

Distance (ft)	Averaged RSSI (dBm)
10	-44
20	-45.5
30	-44.5
40	-48.25
50	-49
60	-56.25
70	-54.75
80	-58.5
90	-58
100	-61.5
110	-60
120	-64.5
130	-66
140	-70.25
150	-70.25
160	-73.25
170	-74
180	-77
190	-78.25
200	-80 unable to reliably connect to node

The averaged RSSI values observed for 16 runs conducted over four days had a standard deviation of four in each of the distinct distance bins between 10 ft and 150 ft. The uniformity of the logarithmic relationship between distance and RSSI measurements was quite unexpected. At distances over 150 ft, the RSSI values fluctuated more broadly.

a. RSSI Measurement Calibration

The controlled experiment performed for phase one was successful in determining the feasibility of using this approach for distance approximation in an

outdoor environment. The actual distance versus averaged RSSI values is shown in Figure 8 and is a close match to a linear curve fit between RSSI(dBm) and distance. The expected relationship is that power is inversely proportional to the square of distance, and by utilizing Matlab's curve fitting toolbox on the empirical data we get

$$RSSI(dBm) = -29 \times \log_{10}(distance\ ft) - 5.7. \quad (3)$$

In examining Figure 8, we see that there is some drop off in the most distant measurements, but relates distance to RSSI values quite well and was utilized in test phase three for computing distances to the collection platform from the unknown nodes.

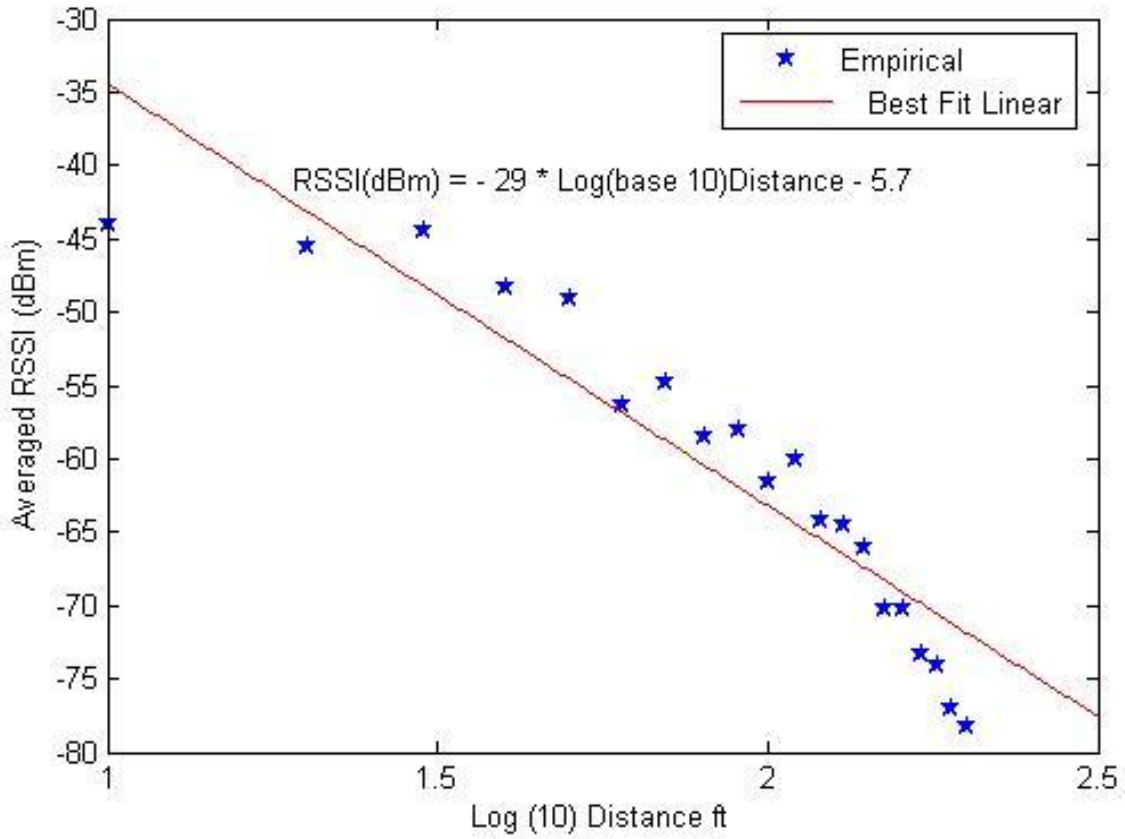

Figure 8. Linear curve fit for RSSI compared to distance.

2. TEST PHASE TWO

In analyzing the results from the tests run in phase 1, the ability of a node to associate with the access point and to hold the connection robustly declined at a distance of 180 ft or greater. The approach was then altered slightly to keep the test environment within the 180 ft constraints. In the earlier phases, the wireless platform provided excellent run-times in excess of four hours but running the necessary router routines provided to be manually intensive. Each time the platform was powered ON, there was a wait time of many minutes while the GPS unit obtained a lock and provided geolocation fix data. Also, the individual queries to associated devices had to be done individually. To facilitate automatic retrieval of data sets, the Linksys WRT-54GL was configured to run a specific routine at startup which could be controlled remotely via a Secure Shell (SSH) connection. The wake-up procedures are summarized in Figure 9, and the full source code is in the Appendix.

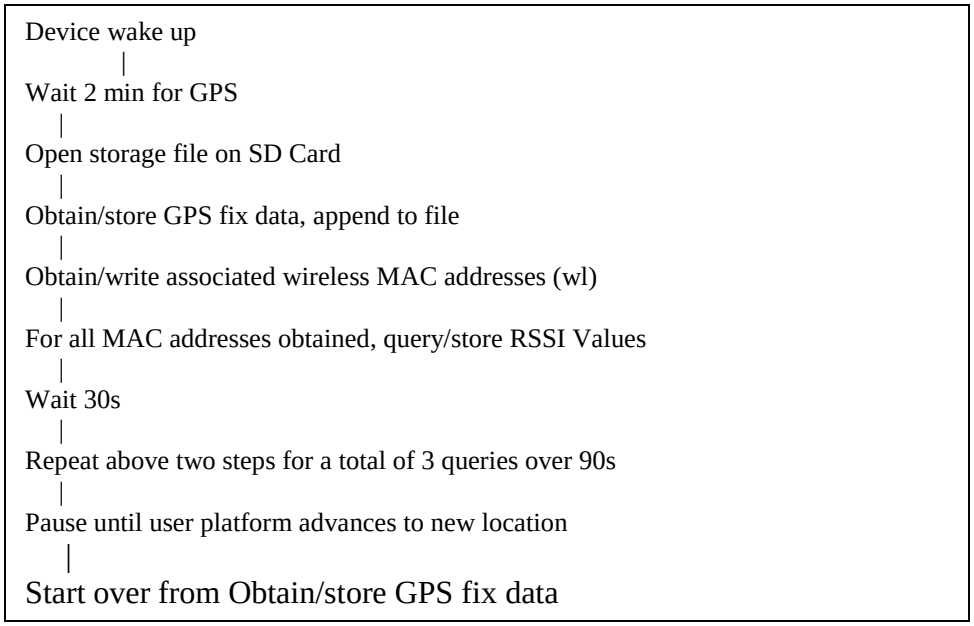

Figure 9. High-level view of data capture routine.

Early analysis of the results from phase two testing confirmed that the wireless nodes utilized were configured automatically and associated to nearby wireless access points via dynamic host connection protocol (DHCP); the connection is reset when power is cycled. This allowed for dynamic placement of devices in the test environment in a layout as shown in Figure 10. Blue triangles represent the placed nodes, and the travel path of the collection platform is drawn in red. In observing the calibration data from testing during phase one earlier, it is observed that RSSI values were reported back in a rounded whole number. This allowed for some overlap of distinguishable values when distances were measured in intervals of less than 10 ft. This prescribed that an efficient path through a given area could be created by dividing the area into 10 ft × 10 ft grids with a simple flight path dictated by turn radius of the collection platform. The receiving unit, was walked the along the prescribed path and interleaving was minimized when possible.

Figure 10. Node placement and query path.

3. TEST PHASE THREE

The second phase of testing allowed for fine tuning of collection methodologies. During phase three, wireless nodes were placed in 180 ft × 60 ft field with locations depicted in Figure 11 as red triangle marks.

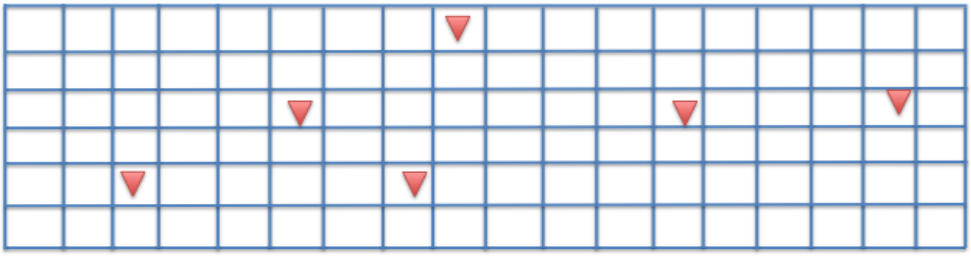

Figure 11. Node placement.

Final test runs were conducted over a three day period with modified parallel track search patterns while keeping the spacing between tracks at 10 ft. At each collection stop along the path, RSSI measurements were obtained from all target nodes, and GPS time stamps were recorded, which allowed for retracing offline to verify full data sets were obtained and to calculate actual distance to nodes from GPS offset measurements. Figure 12 is an error plot which was created to compare the actual distances measured to the calculated distances between nodes and receiver. The calculated distances were obtained by using the best fit linear relationship established in test phase one and the averaged RSSI values from four runs. The red line in Figure 12 represents a 1:1 match, where actual distance from sensor node to access point matches the calculated distance.

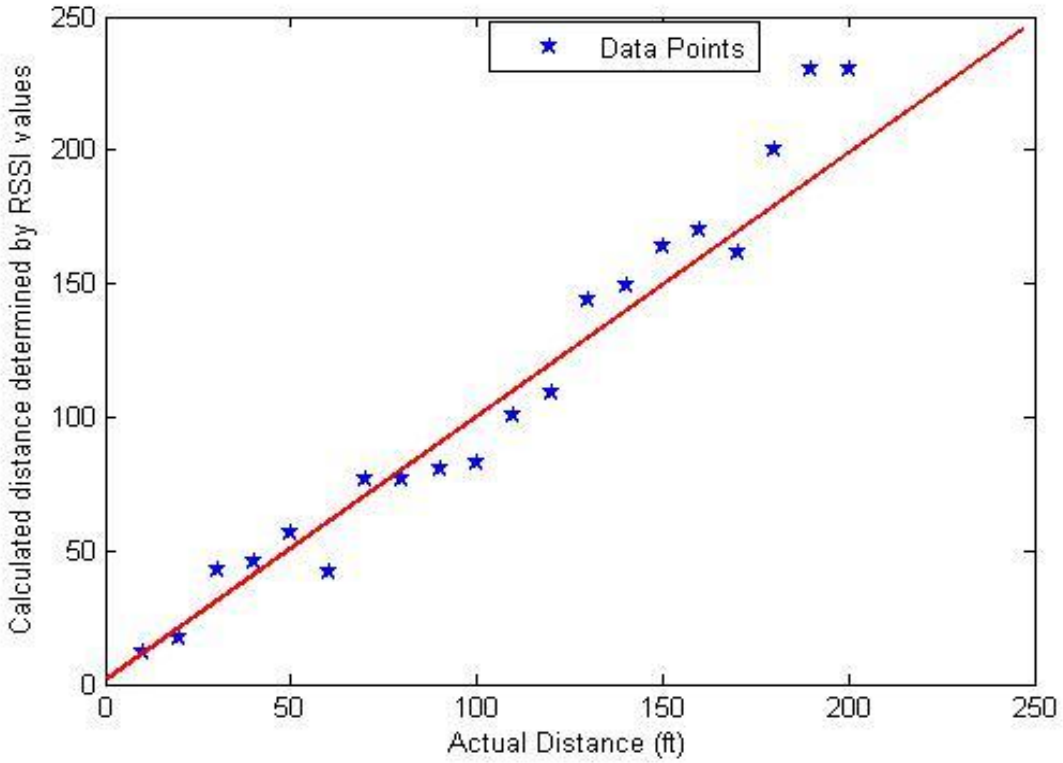

Figure 12. Error plot, actual distance versus calculated.

B. ANALYSIS

The experiment generated a good set of calibration data that was utilized to predict wireless nodes on an 180 ft × 60 ft grid. This overall size of the grid was reduced from earlier estimation due to the limitations of the calibration data to provide meaningful differences at distances greater than 180 ft. Taking extra collection passes through the collection field might mitigate this effect of the limited distance resolution. The calibration equation was used to determine the accuracy of data collected in the third test phase and analyzed for error. The results demonstrated an average accuracy error of 15% for calculated distances with a standard deviation of 3.3 ft. An important observation is that this test was limited to a grid divided into 10 ft × 10 ft plot areas, where the target emitter could reside anywhere within the gridded plot area.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE WORK

In this thesis, a system composed of off-the-shelf components was created to allow for an automated survey of an IEEE 802.11g wireless sensor network. The wireless survey device was controllable from any wirelessly attached client. In that regard, the original question of the feasibility of creating such an automated surveying tool is immediately solvable. The ability to modify a COTS wireless access point to provide an all-in-one solution is a powerful asset that can be used as a very inexpensive leave behind or throwaway collection system. With little rework, such a system can be deployed in an aerial platform or embedded covertly into existing infrastructures for use in any network or wireless sensor node architecture. The collection platform created is small and automated. It has the ability to run off internal power for multiple hours. By limiting the collection of RSSI data to an outdoor line-of-sight environment, it was feasible to correlate RSSI measurements into distance estimations within the accuracies needed for plotting wireless nodes within 10 ft^2 gridded locations. The percentage of error was observed to decrease slightly with increased data sets. Follow-on work of examining this approach in order to create a fully self-guided collection platform, such as a radio-controlled helicopter with the Linksys WRT-54GL attached underneath, would be interesting. Additional work to take received distance estimations from the platform to create overlapping isochrones would be the next logical step to create a fully GPS fixed trilateration map of wireless sensor nodes.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. EQUIPMENT ROUTINES

```
echo "Getting ready to record data to SD Card slot"
sleep 1
echo "Starting up ....."
for i in 1 2 3 4 5 6 7 8 9 10
do
echo -e " \nIteration $i, collecting data....\n\r"
./mmc/thesis/slpkll&  #need this to kill telnet session
telnet 192.168.1.123 10001 > /mmc/thesis/overgps.txt #overwrite file with new data
sed -n '/GPGGA/{p;q;}' /mmc/thesis/overgps.txt > ./mmc/thesis/datastp.txt
echo -e "\r\nGrabbed GPS fix data, next need to query RRSI values for devices\n"
echo ',' >> ./mmc/thesis/datastp.txt
wl assoclist | awk '{print tolower($2)}' > ./mmc/thesis/assoclst.txt
for MAC in `wl assoclist | cut -d ' ' -f 2`
do
  echo -n `cat ./mmc/thesis/assoclst.txt | awk '{x=toupper($0); print x}' | grep $MAC | cut -d ' ' -f 3` > ./mmc/thesis/rssilst.txt
  echo -n ',' >> ./mmc/thesis/rssilst.txt
echo "sleeping" sleep 10
  echo -n `wl rssi $MAC | cut -d ' ' -f 3` >> ./mmc/thesis/rssilst.txt
  echo -n ',' >> ./mmc/thesis/rssilst.txt
  sleep 5 echo -e "sleeping \r\n"
  echo -n `wl rssi $MAC | cut -d ' ' -f 3` >> ./mmc/thesis/rssilst.txt
  echo -n ',' >> ./mmc/thesis/rssilst.txt
  sleep 5 echo -e "sleeping \r\n"
  echo -n `wl rssi $MAC | cut -d ' ' -f 3` >> ./mmc/thesis/rssilst.txt
  echo -n ',' >> ./mmc/thesis/rssilst.txt
done
cat ./mmc/thesis/datastp.txt ./mmc/thesis/rssilst.txt  > ./mmc/thesis/outdata.txt
cat ./mmc/thesis/outdata.txt | tr -d "\r \n" >> ./mmc/thesis/clndata.txt
echo -e "\r" >> ./mmc/thesis/clndata.txt
echo -e "\n\rYou may now go to the next location\r\n"
sleep 2
echo -e "Quickly go to the next location...\r"
echo -e ". \r"
sleep 2
echo -e ".. 10\r"
sleep 2
echo -e "... 9\r"
echo -e "..... 1\r"
echo -e "\r\nAt new location and repeating procedures... \r\n"
done
printf
"GGA,UTC,LAT,LON,FIX_Q,N_SATS,HORZ_DILU,ALT_M,GEOID_HT,SECS_LAST,DGPS_ID,*CHKSUM,EA_ADX,RSSI_1,
RSSI_2,RSSI_3," > ./mmc/thesis/flhdr.txt
echo -e "\r" >> ./mmc/thesis/flhdr.txt
cat ./mmc/thesis/flhdr.txt ./mmc/thesis/clndata.txt > ./mmc/thesis/done.txt
echo -e "Deleting old working files\r\n"
rm ./mmc/thesis/overgps.txt rm ./mmc/thesis/datastp.txt
rm ./mmc/thesis/assoclst.txt rm ./mmc/thesis/rssilst.txt
rm ./mmc/thesis/outdata.txt rm ./mmc/thesis/clndata.txt
rm ./mmc/thesis/flhdr.txt
mv ./mmc/thesis/done.txt ./mmc/thesis/`date '+done_%H%M'`.txt #or `date '+file_%Y%m%d_%H%M'`.txt
echo -e "\n\rData saved to ./mmc/thesis/`date '+done_%H%M'`.txt\r"
echo -e "\n\rDone, you must close SSH window\r"
exit 0
```

Figure 13. Main routine run from SSH connection.

GGA,UTC,LAT,LON,FIX_Q,N_SATS,HORZ_DILU,ALT_M,GEOID_HT,SECS_LAST,DGPS_ID,*CHKSUM,EA_ADX,RSSI_1,
RSSI_2,RSSI_3,

$GPGGA,143433.586,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4A,00:19:4F:D4:F4:8E,0,0,0,

$GPGGA,144024.386,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*49,00:19:4F:D4:F4:8E,-7,-7,-7,

$GPGGA,144055.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4C,00:19:4F:D4:F4:8E,-7,-7,-16,

$GPGGA,144126.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*49,00:19:4F:D4:F4:8E,-16,-16,-16,

$GPGGA,144157.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4F,00:19:4F:D4:F4:8E,-16,-25,-25,

$GPGGA,144228.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*44,00:19:4F:D4:F4:8E,-25,-25,-25,

$GPGGA,144259.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*42,00:19:4F:D4:F4:8E,-33,-33,-33,

$GPGGA,144329.986,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4D,00:19:4F:D4:F4:8E,-33,-33,-33,

$GPGGA,144400.986,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*41,00:19:4F:D4:F4:8E,-42,-42,-42,

$GPGGA,144431.787,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4C,00:19:4F:D4:F4:8E,-42,-42,-42,

$GPGGA,144502.586,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4E,00:19:4F:D4:F4:8E,-51,-51,-51,

$GPGGA,144533.386,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4A,00:19:4F:D4:F4:8E,-51,-51,-51,

$GPGGA,144604.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4E,00:19:4F:D4:F4:8E,-60,-60,-60,

$GPGGA,144635.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4C,00:19:4F:D4:F4:8E,-60,-60,-60,

$GPGGA,144705.986,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*47,00:19:4F:D4:F4:8E,-69,-69,-69,

$GPGGA,144736.787,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*48,00:19:4F:D4:F4:8E,-69,-69,-69,

$GPGGA,144807.586,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*46,00:19:4F:D4:F4:8E,-69,-69,-69,

$GPGGA,144838.586,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4A,00:19:4F:D4:F4:8E,-69,-69,-69,

$GPGGA,144909.386,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*4F,00:19:4F:D4:F4:8E,-69,-69,-69,

$GPGGA,144940.187,8960.0000,N,00000.0000,E,0,0,,137.0,M,13.0,M,,*41,00:19:4F:D4:F4:8E,-69,-69,-69,

Figure 14. Sample data during test 2, collected and stored on SD card.

GGA	UTC	LAT	LON			FIX_Q	N_SATS	HORZ_DILU
$GPGGA	162341.6	3635.871	N	12152.2	W	1	8	1
$GPGGA	162624.4	3635.8727	N	12152.2	W	1	10	0.91
$GPGGA	162655.2	3635.8753	N	12152.2	W	1	7	1.09
$GPGGA	162726	3635.8732	N	12152.2	W	1	8	1.16
$GPGGA	162756.8	3635.8703	N	12152.2	W	1	9	1.12
$GPGGA	162827.6	3635.87	N	12152.2	W	1	10	0.9
$GPGGA	162858.4	3635.8695	N	12152.2	W	1	10	0.9
$GPGGA	162929.2	3635.8621	N	12152.2	W	1	9	0.91
$GPGGA	163000.2	3635.8548	N	12152.2	W	1	8	0.99
$GPGGA	163031	3635.8496	N	12152.2	W	1	8	1.17
$GPGGA	162341.6	3635.871	N	12152.2	W	1	8	1.01
$GPGGA	162624.4	3635.8727	N	12152.2	W	1	10	0.91
$GPGGA	162655.2	3635.8753	N	12152.2	W	1	7	1.09
$GPGGA	162726	3635.8732	N	12152.2	W	1	8	1.16
$GPGGA	162756.8	3635.8703	N	12152.2	W	1	9	1.12
$GPGGA	162827.6	3635.87	N	12152.2	W	1	10	0.9
$GPGGA	162858.4	3635.8695	N	12152.2	W	1	10	0.9
$GPGGA	162929.2	3635.8621	N	12152.2	W	1	9	0.91
$GPGGA	163000.2	3635.8548	N	12152.2	W	1	8	0.99
$GPGGA	163031	3635.8496	N	12152.2	W	1	8	1.17
$GPGGA	162341.6	3635.871	N	12152.2	W	1	8	1.01
$GPGGA	162624.4	3635.8727	N	12152.2	W	1	10	0.91
$GPGGA	162655.2	3635.8753	N	12152.2	W	1	7	1.09
$GPGGA	162726	3635.8732	N	12152.2	W	1	8	1.16
$GPGGA	162756.8	3635.8703	N	12152.2	W	1	9	1.12
$GPGGA	162827.6	3635.87	N	12152.2	W	1	10	0.9
$GPGGA	162858.4	3635.8695	N	12152.2	W	1	10	0.9
$GPGGA	162929.2	3635.8621	N	12152.2	W	1	9	0.91
$GPGGA	163000.2	3635.8548	N	12152.2	W	1	8	0.99
$GPGGA	163031	3635.8496	N	12152.2	W	1	8	1.17
$GPGGA	162341.6	3635.871	N	12152.2	W	1	8	1.01
$GPGGA	162624.4	3635.8727	N	12152.2	W	1	10	0.91
$GPGGA	162655.2	3635.8753	N	12152.2	W	1	7	1.09
$GPGGA	162726	3635.8732	N	12152.2	W	1	8	1.16

Figure 15. GPS data collected during test runs and merged with RSSI values.

Distance Ft	Run 1 average	run 2 average	run 3 average	run 4 average
10	-45	-46	-44	-41
20	-45	-46	-46	-45
30	-48	-42	-44	-44
40	-59	-44	-46	-44
50	-53	-48	-52	-43
60	-60	-60	-58	-47
70	-58	-53	-57	-51
80	-61	-60	-60	-53
90	-60	-61	-59	-52
100	-65	-61	-65	-55
110	-62	-63	-59	-56
120	-69	-66	-64	-58
130	-67	-68	-66	-57
140	-70	-68	-65	-61
150	-70	-76	-72	-63
160	-72	-72	-71	-66
170	-69	-73	-77	-74
180	-79	-74	-73	-70
190	-75	-78	-79	-76
200	-81	-80	-80	-72

Figure 16. Averaged RSSI values over four days, four runs per day.

LIST OF REFERENCES

[1] W. Ho, A. Smailagic, D.P. Siewiorek, and C. Faloutsos, "An adaptive two-phase approach to WiFi location sensing," *4th Int. Conf. on Pervasive Computing and Communications Workshops*, Pisa, Italy, 2006, pp. 452–456.

[2] Chun-Dong Wang, Ming Gao, Xiu-Feng Wang, "An 802.11 based location-aware computing: Intelligent guide system," *1st Int. Conf. on Communications and Networking in China*, Beijing, China, 2006, pp. 1–5.

[3] Gang Zhou, Tian He, Sudha Krishnamurthy, and John A. Stankovic, "Impact of radio irregularity on Wireless Sensor Networks," *Proc. of the 2nd Int. conf. on Mobile systems, applications and services*, Boston, MA, June 06–09, 2004.

[4] Saxena, Mohit, Gupta, Puneet, Jain and, Bijendra, "Experimental analysis of RSSI-based location estimation in Wireless Sensor Networks," *Conf. on Communication Systems Software and Middleware and Workshops*, Bangalore, India, June 2008, pp. 503–507.

[5] M. Kanaan, K. Pahlavan, "A comparison of wireless geolocation algorithms for indoor environments," *Proc. IEEE Wireless Communications Network Conf.*, Atlanta, Georgia, March 21–25, 2004.

[6] Institute of Electrical and Electronics Engineers, 802.11, Wireless LAN Medium Access Control, (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band, September 16, 1999.

[7] S. Haykin and M.Moher, *Introduction to Analog and Digital Communications, Second edition*. Hoboken, NJ: John Wiley and Sons, 2007, pp. 448.

[8] T. Locher, R. Wattenhofer, and A. Zollinger, "Received-signal-strength-based logical positioning resilient to signal fluctuation," 6th Int. Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, May 2005, pp. 396–402.

[9] M. E. Tingle, "Performance evaluation of a prototyped wireless ground sensor networks," M.S. thesis, Naval Postgraduate School, 2005.

[10] DD-WRT firmware version 2.4, retrieved from http://www.dd-wrt.com/routerdb/de/download/Linksys/WRT54G-LA/v8/dd-wrt.v24_micro_generic.bin, March 2010.

[11] P. Asadoorian and L. Pesce, *Linksys WRT54G Ultimate Hacking*, Burlington, MA: Syngress, 2007, pp. 25.

[12] 20 Channel SIRF III OEM GPS unit, as seen at, http://www.sparkfun.com/products/465, last accessed on June 10, 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. R. Clark Robertson, Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

4. Professor Weilian Su
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

5. Professor Xioping Yun
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

6. Lieutenant Todd E. Sims, United States Navy
   Naval Postgraduate School
   Monterey, California