SCRAMBLER DETECTOR FOR WIRELESS HOME SECURITY

By

George Schwieters

Maxwell Willis

Yu Guan

Final Report for ECE 445, Senior Design, Fall 2014

TA: Dennis Yuan

10 December, 2014

Project No. 32

Abstract

This report will discuss a device we designed as an add on to an existing wireless home security system with the purpose of detecting whether or not someone is trying to jam the security system. We will cover the goals we had for the project as well as the overview and features of our system. It also discusses the individual parts that we chose and why they were chosen. This will include the specs of the components, how they form the requirements and verifications of the system, and the total cost to build the system. To close the paper, we will explain tests we performed on the system, problems and successes we had in the process, and lastly how we could expand on this project after our initial design.

Table of Contents

1 Introduction 1

1.1 Design Goals 1

1.2 Project Functions 1

1.3 Project Overview 1

2 Design 4

2.1 Hardware 4

2.1.1 RF Transceiver 4
2.1.2 GSM Module 4
2.1.3 Microcontroller 5
2.1.4 Keypad 5
2.1.5 Alarm 6
2.1.6 Power Supply 6

2.2 Software (Microcontroller) 8

2.2.1 Ping-ack Protocol 9
2.2.2 Pseudorandom Number Generator 10
2.2.3 Data Encryption 10
2.2.4 Freshness Check 11
2.2.5 Power Monitoring 11
2.2.6 Finite State Machine 11
2.2.7 Software Debouncer 12

2.3 Software (Mobile App) 13

2.3.1 iPhone 13
2.3.2 Android 13

3 Design Verification 14

3.1 Master 14

3.1.1 RF Transceiver 14
3.1.2 GSM Module 14
3.1.3 Microcontroller 14
3.1.4 Keypad 15
3.1.5 Alarm 15
3.1.6 Power Supply 15

3.2 Slave 16

3.3 Extra Test 16

3.3.1 Start topology & Ping-ack Protocol 16
3.3.2 External Oscillator 16
3.3.3 Jamming Detection 16

4 Costs 17

4.1 Parts *17*

4.2 Labor *17*

4.3 Total Cost *17*

5 Conclusion **18**

5.1 Accomplishments *18*

5.2 Uncertainties *18*

5.3 Ethical considerations *19*

5.4 Future work *20*

References **21**

Appendix A Requirement and Verification Table **22**

Appendix B Software Flowchart **28**

Appendix C Data Encryption Algorithm - TEA **32**

Appendix D Verification Tools **34**

D.1 ZENA Wireless Adapter *34*

D.2 USB to Serial Converter *34*

Appendix E Mobile App User Interface **35**

Appendix F Test Results **36**

Appendix G PCB Diagrams and Layouts **41**

Appendix H Cost Table **51**

1 Introduction

This project was designed around the idea that current wireless home security systems have multiple crucial vulnerabilities. Most importantly, the central node of current wireless home security systems only listens passively to alert messages sent via radio frequency (RF) channels from sensor nodes when a possible threat is detected. A burglar could use a RF signal jammer to block the alert messages, rendering the system useless. Also, backup power is not standard in wireless home security systems, so the system will cease to function when there is a power outage. In this case, a burglar could simply cut the power lines before breaking into the house in order to circumvent the security system. We will be designing a system to work along with a generic wireless home security system with auxiliary inputs so that together the two systems form a more robust home security system that customers can trust.

In the following sections, the design decisions we have made while designing and building the system will be explained in details, as well as the actual implementation of the system. Then, the test results from the verification procedures will be discussed and the total cost of this project will be estimated. We will then conclude with our accomplishments, uncertainties, ethical considerations and lastly with possible future work. We will emphasize the difficulties we had in this project and propose ideas for how we could fix these issues if we continued working on this system.

1.1 Design Goals

Designing the system, we bear the following goals in mind.

- Create a system that is compatible to available wireless home security systems
- Implement our system to a level of sophistication such that the system is invulnerable to popular attack methods
- Keep the hardware design simple in order to keep cost down

1.2 Project Functions

The final product will have the following functions.

- Use RF transceivers to wirelessly communicate between multiple nodes in the system
- Use a ping-ack protocol to continuously verify communication channels are unobstructed
- Use an encryption algorithm to prevent eavesdropping
- Use a pseudorandom number generator to check message freshness and prevent replay attacks
- Use a Global System for Mobile (GSM) module to send text message to the owner of system to signal a potential threat
- Use a buzzer to auditorily alert the owner of system of a potential threat
- Use a keypad to enable and disable the alarm of the system
- Use batteries as the backup power source to keep the system functioning during power outages

1.3 Project Overview

There are RF signal jamming detection methods where the strengths of RF signals on certain bands are monitored and if the signal strengths exceed a threshold, an alarm is triggered. These methods can detect RF signal jammers in general. However, they tend to produce false positives when the threshold

is set too low, and produce false negatives when the threshold is set too high. Therefore, these methods are not optimal in a security application.

Since the primary function of our system is to detect jammers that can disrupt communication in wireless home security systems, our system employs a different detection method. Our system has a central master node, and several slave nodes. These nodes communicate with each other using the same sub-GHz Industrial, Science and Medical (ISM) bands wireless home security systems use. Our system is configured to be more easily jammed compared to wireless home security systems to ensure that when a jammer disrupts communication in wireless home security systems, communication in our system is jammed as well. When a jammer is not able to disrupt communication between nodes in our system, the jammer is not able to disrupt communication in wireless home security systems either, thus the wireless home security systems will detect intrusions. Although our method of detecting jamming devices produces false negatives, it is still admissible since the wireless home security system will be working. On the optimistic side, this method does not produce false positives.

Subsequently, our system employs a star topology where the master is responsible for communicating with each slave, while slaves do not communicate with each other. Figure 1 demonstrates the star topology in the overall system block diagram, with arrows indicating direction of communication between blocks. Figure 2 and Figure 3 give a high level description of what is inside the master and slaves, respectively.

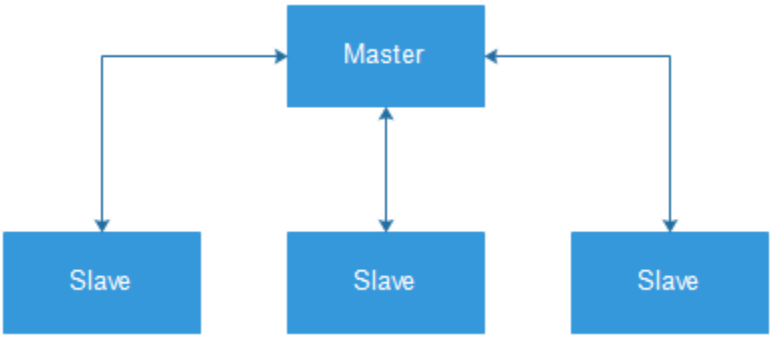


Figure 1 Top Level Block Diagram

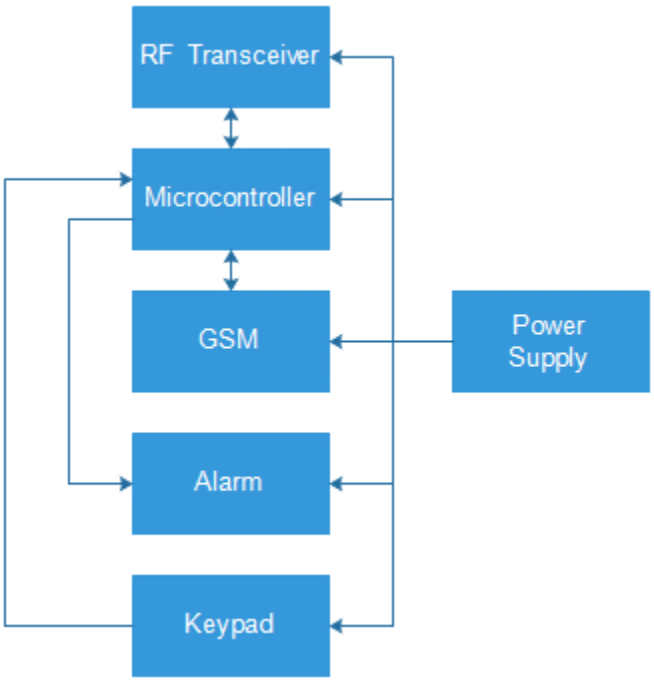


Figure 2 Master Block Diagram

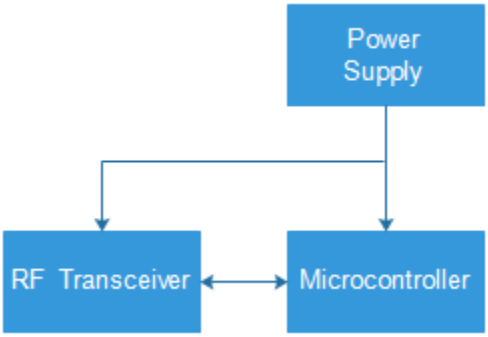


Figure 3 Slave Block Diagram

Master:	Communicates with slaves and user.
Slave:	Responds to master's pings.
Power Supply:	Provides power to all other modules.
RF Transceiver:	Facilitates communication between master and slaves.
GSM:	Sends alerts and receives commands via text messages.
Microcontroller:	Integrates all other modules in to a system.
Alarm:	Signifies a detected potential threat.
Keypad:	Implements a simple user interface.

2 Design

The design procedure as well as the final design for both hardware and software will be presented in detail in this section. We started designing hardware and software for the system simultaneously since they have mutual effects on the design decisions we make. Despite this fact, hardware design will be explained first, followed by software.

2.1 Hardware

We started the hardware design process with choosing specific models for the RF transceivers and the GSM module. Then the microcontroller was selected based on the functions needed. The output power and voltage level for the power supply module was decided afterwards. Design for the keypad and alarm module was done at the end.

2.1.1 RF Transceiver

In order to implement the ping-ack protocol, master and its slaves need to communicate in both directions. Therefore, RF transceivers are needed.

Understanding that all the members on the team lack experiences with RF circuit design, and RF transceivers are not at the core of our project, we searched for development boards that operate in the sub-GHz ISM band in order to avoid designing the circuit ourselves. As it turns out, there are very few choices available. Microchip and Semtech have the best RF transceiver development boards that operate in 433MHz, 868MHz, and 915MHz bands. However, the boards from Semtach cost more than $60, which is too expensive to use in a low cost system, while the RF transceiver boards from Microchip cost less than $10.

Microchip also has developed a MiWi protocol library to be used with their RF transceivers. The library implements a lightweight network protocol stack in contrast to the heavy XBee protocol. The library also supports star topology and data encryption, which will greatly decrease the amount of effort needed to develop the system.

Microchip has two integrated circuit (IC) chips that can be used in our system. The MRF45XA chip operates in all three ISM bands and do not have any development board built using it, whereas the MRF89XA chip only operates in 868MHz and 915MHz band and has development boards [1]. Since we did not plan to build RF circuits, MRF89XA was chosen. MRF89XAM8A and MRF89XAM9A are the two development boards. MRF89XAM8A operates in the 868MHz band while MRF89XAM9A operates in the 915MHz band [2]. Although we used the MRF89XAM8A board in our system, MRF89XAM9A can be easily swapped in, since the two boards has the exact pin assignments and therefore are interchangeable.

MRF45XA, on the other hand, has the exact pin assignments as MRF89XA. Therefore, it is easy to build a printed circuit board (PCB) for MRF45XA that is interchangeable with MRF89XAM8A and MRF89XAM9A.

2.1.2 GSM Module

We decided to use a GSM Module instead of a GSM IC chip since this module is not at the core of our design. There is a variety of choices for the GSM module. We avoided modules with large sizes, high

prices, and excessive features, e.g. SparkFun SM5100 development board. We also avoided modules designed and assembled by unrecognizable entities, e.g. SIM900 development board. We then ended up with the GSM Click board by Mikroelectronika.

2.1.3 Microcontroller

Since we decided to use RF transceivers and the libraries from Microchip, we needed a low-end microcontroller from Microchip that supports the MiWi library. PIC18 series were the least powerful microcontrollers that support the MiWi library.

In order to decide on the microcontroller, we have listed all the required features in a table shown in Table 1. From the table we can see that the microcontroller needs to have more than 29 pins, excluding the power and ground pins for the microcontroller. Therefore, it is obvious that we will need a microcontroller that has at least 29 pins with 3 external interrupts, 4 interrupt-on-change ports, 1 analog pin, 1 Serial Peripheral Interface (SPI), and 1 universal asynchronous receiver/transmitter (UART) interface. None of these needed features should share the same pin.

Table 1 Microcontroller Features Needed

For	Features	# pins
RF transceiver	SPI	3
	Interrupt	2
	Digital I/O	3
GSM module	UART	2
	Interrupt	1
	Digital I/O	4
Keypad	IOC	4
Buzzer	Digital I/O	1
Primary & secondary external oscillator	Digital I/O	4
Light emitting diodes (LEDs)	Digital I/O	3
Power monitor	Analog I/O	1
	Digital I/O	1
	Total	29

Moreover, since the GSM module needs 3.3V as power supply, and the RF transceiver needs 2.1V to 3.6V, we wanted a microcontroller with the same operating voltage level. Subsequently, PIC18F45J10 was selected [5].

2.1.4 Keypad

One of the ways the user interfaces with the system is with the keypad. This simple device is composed of four push buttons that are powered by the power supply module. These are software debounced and connect to the interrupt-on-change ports of the microcontroller module. This allows the button logic to be interrupt driven rather than polled which is advantageous because the microcontroller module's resources are being utilized to its full extent with the Microchip Application Library code that is running on which will be explain in further detail in a separate section.

2.1.5 Alarm

The alarm module will simply be an externally driven buzzer controlled with a low side metal–oxide–semiconductor field-effect transistor (MOSFET) driver. It's not powered by the main output of the power supply module. Instead it's powered by the unregulated input power which can either be the wall adapter or the batteries. The microcontroller GPIO ports for the most part cannot sink or source much current so having it externally powered allowed us to choose whichever buzzer we wanted regardless of current draw. Lastly, initially we decided on sourcing a loud buzzer like one would expect to see in a commercial security system but we later decided to get a far quieter one since that's all we really needed to meet our design goals.

2.1.6 Power Supply

The power supply module consists of a voltage regulator circuit, a wall adapter, three AAA batteries and a simple circuit for switching from wall to battery power in the absence of wall power. This module supplies power to the microcontroller module, GSM module, RF transceiver module, alarm module and keypad module. To keep our design simple we didn't create a transformer for the wall power. We purchased a 5V rectified wall adapter rated high enough to power all of our modules.

Table 2 Power Requirements

Module	Maximum Current Draw (mA)	Minimum Voltage (V)	Maximum Voltage (V)
Microcontroller	17.5	2.7	3.6
RF Transceiver	30	2.1	3.6
GSM	2,000 / 360	3.22	4.5
Alarm	8	3	20
Keypad	2	-	35
Total	2,057.5 / 417.5	3.22	3.6

The above values, shown in Table 2, were used to design the basics of the power supply. From the minimum and maximum voltages we decided to use a generic 3.3V linear voltage regulator. After deciding on the voltage output we looked for a regulator that can handle the full capabilities of the GSM chip so we decided to find something that will handle the 2A spikes in current draw. Next we had to ensure the ripple voltage would be satisfactory for all the modules so we used the regulator's datasheet as a good start. From there we took the minimum requirements in the datasheet for a stable output and added a margin of safety. This was not optimized but that's not a part of our design goals.

Next for the backup power we decided that we only need the master to be powered for a maximum of 1 hour in order to sound the alarm and alert the user via SMS. For this we excluded the 2A current bursts for the GSM chip. This only occurs during voice calls and we only care about the less power intensive data mode for backup power design. From there chose to use three AAA batteries.

$$V_{dropout} = 3.45V,\ V_{batt\ min} = 1.15V = V_{dropout} / 3 \quad (1)$$

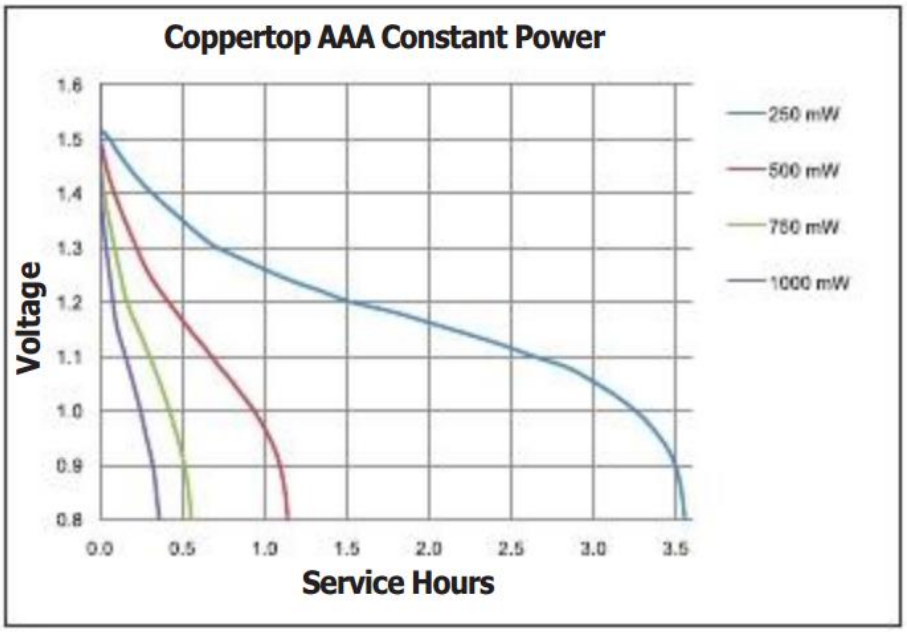


Figure 4 Battery Life

As seen in the equations above and using data from the battery datasheet [6] for the Ah rating and the regulator datasheet [7] for the dropout voltage will have roughly 30 minutes of backup power with everything running. If we consider that the GSM chip only sends a few message then we can scale down the current draw immensely and safely say that 1 hour of constant operation is achievable.

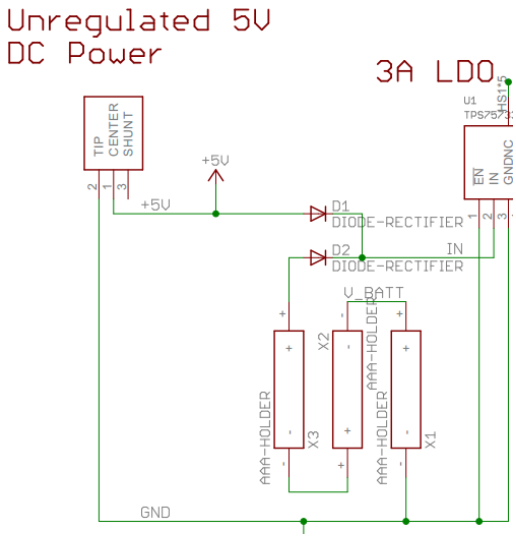


Figure 5 Power Switching Circuit

Next for the wall adapter we simply had to find a product that could support our current draw requirements and the dropout voltage requirement of the regulator. In order to use the simple power switching circuit (Figure 5) we decided to use an adapter that has an output voltage greater than the

backup power but not so high that the linear regulator dissipates too much heat. This led us to use a 5Vwall adapter capable of supplying 2.5A.

And as mentioned previously, Figure 5 shows the power supply switching circuit which is composed of two diodes. These allows the unregulated power input with the highest voltage to supply all the current when both are present. Then when the higher voltage power input is removed the other power input takes over.

Lastly we investigated the expected power dissipation of the linear regulator. Here are calculations for the expected power dissipation for the regulator chip. Since the GSM module has the ability to sink 2A of current we decided to design for the capabilities of the GSM for safety even though we don't plan on performing voice calls. In the calculations below we examine the power dissipated for 2A of continuous draw and then the power dissipated during normal operation for comparison.

$$P_D = (V_I - V_O) * I_O + V_I * I_Q P_D = (V_I - V_O) * I_O + V_I * I_Q \quad (2)$$

$$V_I = 5V, \quad V_O = 3.3V, \quad I_{O\max} = 2.06A, \quad I_{Oavg} = 420mA, \quad I_Q = 200\mu A \quad (3)$$

$$P_{Dmax} = 3.5W, \quad P_{Davg} = 0.72W \quad (4)$$

$$T_J = T_A + P_{Dmax} * (R_{\theta JC} + R_{\theta CS} + R_{\theta SA}) \quad (5)$$

$$T_A = 40^{\circ}C, \quad R_{\theta JC} = 2^{\circ}C/W, \quad R_{\theta CS} = 0^{\circ}C/W, \quad R_{\theta SA} = 18^{\circ}C/W \quad (6)$$

$$T_{Jmax} = 110.1^{\circ}C, \quad T_{Javg} = 54.3^{\circ}C, \quad R_{JA} = 20^{\circ}C/W \quad (7)$$

As seen in the calculations above, the junction temperature in both cases is within the operating temperature range of the device which is -40 to 125°C. The junction temperature for when a little over 2A is being sourced is a little on the hot side, but this condition will be seen rarely since it is only a burst current that the GSM module is sinking, and the GSM module does not always need to sink that much current to operate. And now looking at the normal operation heat dissipation we can see that the regulator will operate fine.

2.2 Software (Microcontroller)

Interfaces between the microcontroller and all the peripherals were established by software. The software initializes all the peripherals, sets up the star topology, and performs the main work load which includes a ping-acknowledge (ping-ack) protocol. Figure 7 in Appendix B shows the software flowchart for the generic main function that is common in both master and slave. Then Figure 8 through Figure 11 expand the subroutines. Note that only flowcharts at higher levels are provided for readability.

In order to make our system secure, we not only needed to detect jammers and power losses, but also we needed to prevent replay attacks, eavesdropping and spoofing. Table 3 shows the possible threats

and the corresponding prevention and detection methods used. In the following sections, these methods will be explained in details.

Table 3 Threats and Prevention/Detection Methods

Possible threats	Prevention/detection methods
Jammers	Ping-ack protocol
Power cuts	Power monitoring Ping-ack protocol
Replay attack	Freshness check
Eavesdropping	Data encryption
Spoofing	Pseudorandom number generator

2.2.1 Ping-ack Protocol

Initially we wanted to implement a heartbeat protocol where a slave pings the master periodically so that the master can keep track of the time elapsed since the last ping received. When the master does not receive ping from one slave for a while, the master will mark that slave as dead and raise an alarm. We then realized that when slaves ping the master periodically, it is possible that multiple slaves transmit packets at the same time and cause crosstalk interference. As a result of the interference, the master may mistakenly disregard the heartbeat packets, mark the slaves as dead and raise an alarm, which is undesirable.

To prevent crosstalk interference, we can either implement a time synchronization algorithm to keep the time on all nodes consistent, or serialize the communications so that only one node transmits packets at any time. For implementing either method, two-way communication channels will be needed, meaning RF transceivers are required. Since a stable synchronization algorithm requires a considerable amount of effort that exceeds its payoffs, we decided to use a ping-ack protocol.

In a ping-ack protocol, a central node as the master is needed. The master is responsible for pinging each of its slaves. The slaves then send back an acknowledgement packet. In order to make our system secure, multiple techniques are used along with the ping-ack protocol. A data encryption algorithm is used to encrypt the payload of all the packets. Instead of sending out a packet with the payload indicating it is a ping, we have added a seed field to the payload. The seed is generated using the current time recorded by the timer on the master. Then both master and slave will feed the seed to a pseudorandom number generator to calculate the next number in the sequence. The slave then generates an acknowledgement packet with the calculated number in the seed field and sends the packet back to the master. The master compares the received number against the computed number. If the two numbers match, the master will generate another seed using current time, and ping the next slave. It the two number do not match, or no acknowledgement packet is received within a certain amount of time, the master will deem that slave as dead and raise an alarm. Table 4 shows the ping-ack protocol.

Table 4 Ping-ack Protocol

Time Slot	Master		Slave1	Slave2
1	Send seed	---------->		
2	Calculate number N1 using seed		Calculate number N2 using seed	
3		<----------	Send number N2	
4	Compare N1 & N2			
5	Send seed	---------->		
6	Calculate number N3 using seed			Calculate number N4 using seed

The ping-ack protocol itself detects effective jammers working in adjacency, as well as power losses on slaves. The reason is that jammers and power losses on slaves will both stop the slave from returning acknowledgement packet to the master, therefore the master will mark the slaves as dead and raise an alarm.

2.2.2 Pseudorandom Number Generator

The pseudorandom number generator (PRNG) used is the classic linear congruential generator (LCG) that is defined by the recurrence relation:

$$X_{n+1} = (aX_n + c) \mod m \tag{8}$$

The reason for using LCG is that the algorithm is very low cost which fits the low power profile of the entire system. However, LCG is known to be cryptographically insecure meaning that given enough information, a cryptanalyst can predict X_{n+1} given only X_n. To increase the level of security the system provides, a more powerful microcontroller with hardware random number generator from Microchip can be used. However, under the assumption that the data encryption algorithm is secure enough, it is permissible to use an insecure PRNG algorithm, in order to achieve a low power and low cost system overall.

The PRNG and random seed can prevent sophisticated hackers from spoofing the acknowledgement packets, assuming the data encryption algorithm, TEA, is secure enough so that no information about the LCG is leaked to the hacker.

2.2.3 Data Encryption

The MiWi protocol library uses hardware to perform a low-cost encryption algorithm called the tiny encryption algorithm (TEA) [3]. It is designed for low end microcontrollers, like the 8-bit microcontroller our system uses. In contrast to the typical implementation of Data Encryption Standard (DES), Triple DES and Advanced Encryption Standard (AES), which normally takes up to 4KB of programming space, the typical implementation of TEA only needs several hundred bytes of programming space. In addition, the most secure block cipher mode, Cipher Block Chaining (CBC) mode, is used to maximize the security of

our system. Figure 12 and Figure 13 in Appendix C show the TEA hardware design and the flow diagram for block cipher in CBC mode.

It is possible to increase the security level our system can provide, by using a more powerful microcontroller from Microchip, e.g. PIC24 series has hardware DES and AES abilities. However, since TEA is said to provide comparable security, and be more power and resource efficient. We decided to keep using the PIC18F45J10 microcontroller, bearing the tradeoff of security and efficiency in mind.

The data encryption algorithm is used to prevent sophisticated hackers from intercepting packets exchanged between master and slaves, then actively tries to decode the packets, and finally reproduces the packets.

2.2.4 Freshness Check

The MiWi protocol stack also includes a counter that is incremented for every transmission. Although the value of this counter is not encrypted, it provides a fast and efficient way to detect replay attacks from less sophisticated hackers.

2.2.5 Power Monitoring

Power monitoring is done only on the master by feeding the unregulated 5V output from the power supply to a digital I/O port on the microcontroller, and feeding the positive terminal of the battery that is connected to the ground to an analog I/O pin on the microcontroller. When the wall adapter fails to provide power, the master will keep running using the backup power. Since the input to the I/O port of microcontroller consequently goes to a logic 0, an alarm will be triggered by the master. The master will also periodically poll the voltage across the grounded battery. Assuming the user replace all the batteries at the same time, when the voltage drops below the threshold, one of the LED on the master will be turned on indicating that batteries need to be replaced.

The reference voltages for the analog to digital (A/D) converter is set to be the same as the power levels of the microcontroller, which are the ground and 3.3V DC. The A/D converter has 10 bits, meaning it has a (3300mV-0mV)/1024 = 3.22265625mV precision. Since we want the threshold to be at 1200mV, we are expecting a reading of 1200mV/3.22265625mV = 372.363636. However, the A/D converter only provides integer values, so the threshold should instead be set at an integer close to 372.3. Considering 1.2V on a battery means it is almost died, we want to make sure the battery change indicating LED is turned on before the backup battery is actually dead. Therefore, the threshold is set to be 374. Consequently, the LED should turn on when the battery provides less than 374x3.22265625mV= 1205.27mV.

2.2.6 Finite State Machine

The Finite State Machine (FSM) is used to quickly process data received from the GSM module over UART interface. The UART receiver generates an interrupt when the receiver buffer is full. In the interrupt handler, instead of transferring the data in the receiver buffer to another buffer, we decided to use a FSM to parse the data very efficiently. Table 5 lists the patterns to be recognized. Figure 6 shows a small portion of the otherwise giant FSM, which processes one of the patterns listed in Table 5. The other patterns are recognized using similar FSMs.

Table 5 Patterns to Be Recognized by FSM

Pattern	Meaning
OK\r\n	Command processed correctly, ready for next command
ERROR	Command failed, ready for next command
CREG:	Registration status
CMGL:	List of text messages
DisAlarm	Disarm the alarm on the master
SetAlarm	Trigger the alarm on the master

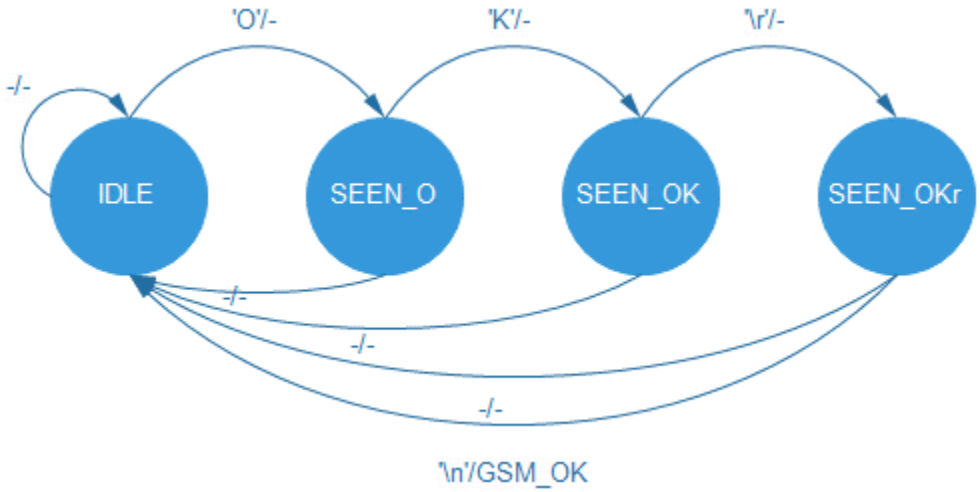


Figure 6 FSM for Pattern OK\r\n

Note that all labels use format input/output. The label -/- denotes default transition where the input is not covered in other cases.

2.2.7 Software Debouncer

The software debouncer is useful for the keypad, since there is not a debouncing circuit build for the buttons. The keypad consists of 4 buttons which are connected to PortB pins on the microcontroller. When a button is pressed the voltage levels on microcontroller pins are changed, and the changes trigger a PortB interrupt-on-change interrupt [5]. Inside the interrupt handler, the IOC feature is first disabled, then an empty for-loop is executed as a delay function so the glitches generated by the buttons are disregarded. Then the voltage level on the pin is captured, and IOC is enabled.

The delay time of the for-loop is influential for the functionality of the system. If the delay is set too high, and user releases the button immediately, the key stock may not be registered. On the contrary, if the delay is set too low, glitches from the buttons may be captured. After testing the delay time, we have reached to a conclusion that a delay of 10ms works the best.

2.3 Software (Mobile App)

The main reason for having a mobile application is that the user of system do not need to memorize the commands for the system and manually send the command text messages. If time permits, a graphical user interface can be built for intuitive control experiences as well.

2.3.1 iPhone

Due to security limitations on the iOS operating system, the mobile application is only able to populate the text message fields on iOS devices, and the user has press the send button in order to send the text message. It is not ideal, but it does eliminate the need for the user to remember the commands. Figure 14 in Appendix E shows the simple user interface we have created.

To circumvent the security measurements, we could use an internet based SMS service for sending the messages. Then the mobile application only needs to send out Uniform Resource Locators (URLs) as commands to the SMS service. Since we could only find commercial services, we decided not to employ this approach.

2.3.2 Android

Theoretically, a mobile app on Android will work perfectly, since there is no security limitation on text messages. Therefore, if time permits, we will be able to build an Android app that integrates with our system seamlessly.

3 Design Verification

We started assembling the system on protoboards and breadboards for proof of concepts. Then we assembled the PCBs. Systematic verifications were done throughout the entire process. In this section, all the tests done will be discussed in details. The requirement and verification table is shown in Table 9 and Table 10 in Appendix A. Appendix D introduces the tools used for verification procedures.

3.1 Master

Master was built on a breadboard for proof of concept. The primary external oscillator was connected first. Then the SPI interface is tested, before connecting the RF transceivers. The UART interface on the microcontroller was verified along with the power source assembled on a protoboard. The GSM module is then attached to the breadboard. Keypad, alarm, and the backup power source are not implemented on the master prototype. The same steps were taken while assembling the master on a PCB. Then keypad and alarm modules are tested. The tests shown in the following section, however, are not in a chronological order.

3.1.1 RF Transceiver

- RF transceivers must correctly receive more than 99% of wireless data sent

While debugging the software for the system, the RF transceivers on master and slaves exchanged well over 100 MiWi protocol packets (over 1000 bits) in order to perform the ping-ack protocol. The microcontroller correctly interprets the received data by the transceiver every time. It is obvious that this requirement is met. Therefore, the actual test was not performed.

- Communicate with another transceiver 20 m ± 5 m away

In order to verify this requirement, we have set up the system with one master and two slaves in the system. We then used a sniffer to monitor the ping-ack protocol that is happening between the nodes. Then we took one of the node away from the other two nodes. When one of the slaves is 23m away from the master, the master failed to receive acknowledgement packets from that slave.

3.1.2 GSM Module

- Receive text messages only from a list of preprogrammed numbers

We verified this requirement by sending correct commands using phone numbers that are not on the list. The system did not respond to the commands.

3.1.3 Microcontroller

- Must be able to output data using SPI protocol correctly more than 99% of the time

Since MRF89XAM8A only supports SPI in 0, 0 mode, which means the clock remains low when idle, and data is captured on positive clock edges, we have programmed the microcontroller to output hard coded data repeatedly. We connected an oscilloscope to the data out and clock ports of the micro controller to verify the output data is correct. Figure 15 in Appendix F shows part of the test result where the data sent is 0x67 shown in green. We repeated this process for 100 times, and every time the result is correct.

- Must be able to output data using UART protocol correctly more than 99% of the time

UART interface needs a fixed data rate, which is set to be 9600 bits/sec by us. We first verified the data rate by connecting the output port of the UART interface to an oscilloscope and programmed the

microcontroller so that it sends out hard coded data repeatedly. Figure 17 shows 104us/bit which is equivalent to 9600bits/sec. We then verified that the UART interface outputs bytes correctly using an oscilloscope again. Figure 18 shows in green the test result when "AT\r\n" was sent on UART. Finally the UART output port is connected to a serial port on computer. Figure 19 shows the data are correctly received by the computer. During these testing procedure, over 100 bytes of data are sent, which were all correctly received, either by oscilloscopes or serial port on computers.

- Must parse data received from the SPI protocol and detect replay attacks more than 99% of the time

One of the slaves were programmed to repeat the first acknowledgement packet, the master raised an alarm every time for 100 times.

- Must finish a round of ping-ack protocol in 3 ± 0.1 seconds
- Must detect Slaves that are unresponsive within 30 ± 1 seconds

The actual speed of the ping-ack protocol without any delay functions is greater than 5 rounds/sec. One round of ping-ack protocol will take less than 0.2 second.

However, transmitting packets at this frequency is not desirable, since our system will be working along with wireless home security systems, if we keep spamming the same frequency band, our system will effectively become a jammer. To lower the transmission frequency, delay functions are needed.

3.1.4 Keypad

- Must be debounced

The microcontroller was programmed so that every time the outputs from the buttons are changed, the microcontroller toggle one LED. We connected an oscilloscope to the power pin of the LED, and did not see any glitches.

- Must be able to recognize correct keys patterns

Random keys were entered to the system, and alarms were triggered. Only when the correct key pattern is entered, no alarm is triggered.

3.1.5 Alarm

- Can be heard clearly from 30 m ± 0.5 m away

For proof of concept, we used a low power buzzer, which cannot be heard from 30m ± 0.5 m away. It is very easy to modify our system to meet this requirement.

- Less than 0.3V should be provided to the Alarm module when it is not triggered

The measured voltage level is 0.26V when the Alarm module is not activated. Therefore, this requirement is met.

3.1.6 Power Supply

- Must supply 3.3V±0.1V DC

The measured output power from our power supply is 3.303V.

- Must be able to withstand a current burst of 2A±0.12A

We connected fourteen 20Ω resistors in parallel which gives us 1.43Ω. Then the resistors are connected to a switch in series. The total resistance is 1.61Ω which draws 2.04966A. We then closed the circuit for

very short amount of time repeatedly to simulate current bursts. After the circuit cools down, we went through all the other requirements to make sure the power supply still works.

- Must continuously supply power to all components connected to it in the event of power outage using the backup battery

When the wall adapter is unplugged, the master does not reset, and continue working.

- In case of power outage, the backup battery must supply power to the system for at least 1 hour

This test is highly dependent on the batteries used. The ones we used for testing were able to keep the master running for more than 1 hour.

- When the voltage from the back up batteries is less than 1.2V ± 0.1V, the Battery Replacement Indicator must turn on

We connected a power source to the first battery slot, and dialed the output voltage from 0.8V to 2.6V. The threshold was at 1.207V. The LED turns on when voltage drops under 1.207V, and turns off when voltage is higher than 1.207V.

3.2 Slave

The requirements for slaves are a subset of that for master. Therefore, the tests done for the slaves are duplicated from the tests shown above. The results of the tests were similar, so they will not be discussed in this section again.

3.3 Extra Test

3.3.1 Start topology & Ping-ack Protocol

Figure 16 in Appendix F shows the master and slaves finishes hand shake and do form a star network in purple. Then the blue entries shows the ping-ack protocol is working.

3.3.2 External Oscillator

Since we used surface mount crystals for the PCBs, which are hard to solder correctly, we needed to check if the frequency is 8MHz when driven by the microcontroller. Figure 23 in Appendix F shows the test result which verified it.

3.3.3 Jamming Detection

We determined if our system does indeed detect jamming, by taking our system into an RF lab and using a signal generator as well as a spectrum analyzer to properly test how our system responds to another signal on the same frequency. What we found out is that our system will detect jamming when the power of the jammer has a power that is 0 to -3dB higher than the output power of our system. We determined that this desirable performance for our system as it won't detect insignificant noise but will trigger when there is a jamming device that would jam a wireless security system.

Figure 24 in Appendix F shows that we have matched the output signal strength of the signal generator to that of our system. Figure 25 in Appendix F shows when we overlapped the signals of our system and the signal generator.

4 Costs

4.1 Parts

Table 6 Costs for Parts

Module	Quantity	PCB Parts Cost ($)	PCB Cost ($)	Total Cost ($)
Master	1	113.17	33.00	146.17
Slave	2	38.96	33.00	71.96
Total		*191.09*	*99.00*	***290.09***

4.2 Labor

Table 7 Costs for Labor

Module	Wage ($/hr)	Total Labor (hr)	Total Cost ($)
George	50.00	200.00	25,000.00
Maxwell	50.00	200.00	25,000.00
Yu	50.00	350.00	43,750.00
Total			**93,750.00**

4.3 Total Cost

Table 8 Total Cost

	Cost ($)
Parts	290.09
Labor	93,750.00
Total	***94040.09***

5 Conclusion

5.1 Accomplishments

At the end of this project we were able to properly detect jamming, spoofing, replay attacks and power loss. The ping-ack protocol that we ran properly calculated and compared the pseudorandom numbers along with the freshness check. We were able to prove this performance when we tested the system. When a jamming signal first started interfering with the system communication the master would start dropping packets. At this point in time we would also get packets in which the random number was incorrect and the system properly detected this and set off the alarm.

We also used a serial port to monitor the communications of the GSM module and we were able to verify that the GSM receives text messages from numbers other than the preprogrammed number, however it properly discards these foreign commands and only responds to commands from the preprogrammed number.

The alarm and keypad system performed as we designed as well. Whenever an incorrect passcode was entered into the keypad, the alarm went off, and when the correct passcode was entered the system deactivated correctly. The GSM also deactivates the alarm when the user sends the “DisAlarm” command.

On a higher level, our system communicates very well within the designed 25 meters. This is when the output power of the transceivers is set to 1dBm. This can be increased to up to 10dBm, which will increase the transmission distance if it is desired. Along with this, it properly detects jamming when the jammer outputs a power that is the same to 3dB’s above the power of the transceiver. This will properly detect a jammer but will also not be set off by arbitrary noise around the system.

The PCB’s were soldered well the first time so that the slave units worked immediately after being soldered. This reduced debugging time as well as time we would’ve had to wait for new boards to come in.

5.2 Uncertainties

One of the main difficulties we had with our system is our master PCB. We were never able to get the RF transceiver on the PCB to talk with the slaves and we never found the problem. We think it may be the fact that both the antenna for the transceiver and GSM are off the same side of the PCB or that the trace from the microcontroller to the transceiver is too long. We were able to eliminate the bit rate as a source of concern because it is relatively low. In order to properly test our system we had resort to our implementation of the master on a breadboard, which is the original build in the designing stage of the project.

We also decided to add a low battery indicator to our code. However, this indicator only measures the voltage across one battery, so this assumes that the user will replace all the batteries at once. To improve this we would measure each individual voltage and set off the indicator when any individual battery is low.

While the keypad properly set off the alarm when an incorrect code is entered and deactivates the alarm when the proper code is entered, you can break the code by spamming the keypad. In this situation, the alarm will continue to go off and the user will not be able to deactivate it short of performing a hard reset.

Lastly, iOS does not allow applications to send text messages directly from the app. Therefore, for iPhones, we designed the app to populate a text message with the correct command to alarm or disalarm the system. All the user needs to do is hit the send button to execute the command. The app was able to automatically send the text message for android users.

5.3 Ethical considerations

The purpose of our project is to create a system that properly detects jamming of a wireless security system. This means that consumers will be relying on this device to protect their house and belongings, but most importantly, themselves and their families. This is a great responsibility therefore we have to be sure that our system does what we say it will do. This goes along with the first item of the code of ethics.

When it comes to item 3, we also must make sure that we do not make outrageous claims in our project that we cannot fulfill. Therefore, we must make sure that we keep our expectations with our project reasonable. We do this by only choosing one frequency to broadcast on and detect jamming. If we were to attempt to detect multiple frequencies it would expand the scale of our project and would introduce other problems.

We will also be learning much more about microcontroller and transceiver integration as well as about GSM's which none of us have dealt with before. We will also be expanding our knowledge of PIC's and using MPLAB. We will learn about the difficulties involved with this and teach us how to adapt to these new difficulties. This lines up with item's 5 and 6 of the code.

In the process, we will seek out peer reviews as well as constructive criticism. Given all the time that we will be dedicating to this project we will get stuck in our ways and having a fresh pair of eyes look at our project and give us suggestions would be greatly appreciated in this process. These suggestions will be accepted regardless of stature and qualifications of the critic. Along these same lines, we should make sure that we are offering our suggestions and criticism to other groups in an attempt to better their projects as well. This follows item's 7, 8, and 10 of the IEEE code.

There are several aspects of our project need to be discussed. The most obvious concern is the potential of electric shock. All electronic devices have the potential to cause an electric shock and even death. As an attempt to prevent it, we have separated the high voltage power source completely from the central part of our system using a simple transformer that converts 120V AC to 5V DC. Although the power source will be able to output 2A current, and more than 100mA current going through human heart may cause death, it is very unlikely that a 5V DC source will induce 100mA current in human body, since according to a study, in the most extreme situation, a path in a human body will have more than 300 ohms resistance. However, even though 300 ohms and 5V will only generate roughly 16mA which is not enough to kill, it is still capable of causing severe pains. Since our project may require extensive human interaction with the system, we have to implement more precautionary measures to prevent electric shocks. Most importantly, we will securely enclose the circuits of our project, so that no part of the circuit will come in contact with human body easily. We will also use waterproof buttons on the keypad, so that even if a person operates the keypad with a wet hand, no water will get into our system and start conducting currents.

Another concern is the potential of fire induced by electronic parts failures. In order to prevent it, we have selected voltage regulators with the ability of thermal and overcurrent shutdown. On top of that, we will also use fuses to doubly make sure that overcurrent will not occur.

The last concern is the potential damage caused by radiations generated from the RF transceiver and GSM modules. In order to minimize the negative impacts of the radiations on human body, we will be using parts that comply with the FCC and IEEE regulations for handheld devices, meaning that our project will cause no more harm than a cellphone or a remote car key, when our system is operating in close range to human body.

5.4 Future work

The key aspect of this project that would need to be focused on in the future would be fixing the master PCB and figure out what was wrong with it. If we could get this aspect of it working it would prove that our system works a whole as well as be a better proof of purpose.

In the future we could expand this jamming detector from being an add-on to being it's own security system. We could incorporate the jamming detector with video cameras, motion detectors and other security system peripherals.

References

[1] MRF89XA Data Sheet. Retrieved from:
http://ww1.microchip.com/downloads/en/DeviceDoc/70622C.pdf

[2] MRF89XAM8A module picture. Retrieved from:
http://static3.tme.eu/katalog_pics/4/b/c/4bc95e7be445b1186a46ce98449aeeef/mrf89xam8a-i_rm.jpg

[3] MiWi Media Access Controller. Retrieved from:
http://ww1.microchip.com/downloads/en/AppNotes/01283a.pdf

[4] ZENA Wireless Adapter User Guide. Retrieved from:
http://ww1.microchip.com/downloads/en/DeviceDoc/70664B.pdf

[5] PIC18F45J10 Data Sheet. Retrieved from:
http://ww1.microchip.com/downloads/en/DeviceDoc/PIC18F45J10%20Family%20Data%20Sheet.pdf

[6] Copper Top AAA battery Data Sheet. Retrieved from:

http://ww2.duracell.com/media/en-US/pdf/gtcl/Product_Data_Sheet/NA_DATASHEETS/MN2400_US_CT.pdf

[7] Voltage Regulator. Retrieved from:

http://www.ti.com/product/TPS75733/technicaldocuments

[8]

Appendix A Requirement and Verification Table

Table 9 Requirements and Verifications for Master

Requirements	Verification	Verified?
Power Supply:		
1. Must supply 3.3V±0.1V DC	1. a. Plug the Power Supply module into the wall and log the output voltage using an oscilloscope for a continuous hour b. The output voltage must fall between 3.3V±0.1V as seen on the oscilloscope	Y
2. Must be able to withstand a current burst of 2A±0.12A	2. a. Plug the Power Supply module into the wall b. Connect a switch and a 1.65Ω resistor in series to the DC output terminals c. Switch on and off the switch in one second. No parts on the circuits should be heating over 110°C d. The circuit should also pass all other tests for Power Supply module after performing this test	Y
3. Must continuously supply power to all components connected to it in the event of power outage using the backup battery	3. a. Plug the Power Supply module into the wall and connect the output to an oscilloscope to draw the V-t plot b. Any module must not have a Power On Reset (POR)	Y
4. In case of power outage, the backup battery must supply power to the system for at least 1 hour	4. a. Put in a new backup battery into the Power Supply module without plugging in the wall transformer b. An audible alarm must be set off, and a text message must be received. The alarm must last for 1 hour straight.	Y
5. When the voltage from the back up batteries is less than 1.2V ± 0.1V, the Battery Replacement Indicator must turn on	5. a. Set up the system normally b. Use a power supply to supply 0V ± 0.1V to 1.6V ± 0.1V to the first battery slot c. The LED should turn on when there is less than 1.2V ± 0.1V and should turn off when it is greater than 1.6V ± 0.1V	Y

RF Transceivers		
1. RF transceivers must correctly receive more than 99% of wireless data sent	1. a. Set up the system normally b. Use the sniffer to broadcast 100 bits of data at 868MHz band using all channel from channel 0 to channel 31 c. Use an oscilloscope to monitor the output from the RF transceivers d. The output must output more than 99 bits of data sent by the sniffer correctly	N
2. Communicate with another transceiver 20 m ± 5 m away	2. a. Place two transceivers next to each other b. Set up the two transceivers to establish a ping-ack protocol c. Use the sniffer to monitor the conversation d. Slowly move the two transceivers away e. Conversation should be disrupted when the transceivers are 20m ± 5m away	Y
GSM		
1. Receive text messages only from list of preprogrammed numbers	1. a. Set up the system normally b. Send a text message to the GSM module using a phone number that is not the designated phone number i. The GSM module should disregard the received text message, meaning that the Microcontroller module should not be able to get a text message from an unknown number	Y

Alarm		
1. Can be heard clearly from 30 m ± 0.5 m away	1. a. Turn on the alarm with someone 30m±0.5m away and measure how loud it is in decibels b. The decibel level must be above 50 dB	N
2. Less than 0.3V should be provided to the Alarm module when it is not triggered	2. a. Set up the system normally b. Use a voltmeter to measure the voltage across the buzzer i. The reading must be less than 0.3V.	Y
Microcontroller		
1. Must be able to output data using SPI protocol correctly more than 99% of the time	1. a. Set up the system normally b. Connect the output of the microcontroller module to an oscilloscope c. Output a 100 bits of data from the microcontroller d. At least 99 bits of data displaying on the oscilloscope must match the data sent.	Y
2. Must be able to output data using UART protocol correctly more than 99% of the time	2. a. Set up the system normally b. Connect Tx and Rx pins to serial port on a computer and use HyperTerminal to monitor the data being transmitted c. At least 99% of characters in the text message received by cell phones must match the preprogram text message	Y
3. Must parse data received from the SPI protocol and detect spoofing attacks more than 99% of the time	3. a. Set up the system b. Use the sniffer to broadcast spoofed data at 868MHz band at all channels from 0 to 31 c. Use an oscilloscope to monitor the output of the RF transceiver d. Verify the SPI interface output from the RF transceiver is correct e. Use a voltmeter to monitor the output level of the AlarmEnable pin	Y

	f. The AlarmEnable pin must be pulled high at most 3 second after the correct data is sent via SPI protocol g. Repeat a to f 100 times h. The test must pass at least 99 times	
4. Must finish a round of ping-ack protocol in 3 ± 0.1 seconds	4. a. Set up the system normally b. Use an oscilloscope to measure the time elapsed from the start of a write to RF Transceiver module to that of the consequent one i. The time elapsed must be less than 3 ± 0.1 seconds	Y
5. Must detect Slaves that are unresponsive within 30 ± 1 seconds	5. a. Set up the system normally b. Unplug or use a metal box to cover one Slave at anytime c. An alarm must be triggered within 30 ± 1 seconds	Y
<u>Keypad</u>		
1. Must be debounced	1. a. Use an oscilloscope to monitor the output level of the LED that is controlled by the keypad through the microcontroller b. Plug the Power Supply module into the wall c. Press every key on the keypad d. There must not be any glitches shown on the oscilloscope	Y
2. Must be able to recognize correct keys patterns	2. a. Set up the system normally b. Trigger an alarm c. Enter random keys and the alarm should not be disarmed d. Enter the correct key and the alarm should be disarmed	Y

Table 10 Requirements and Verifications for Slave

Requirements	Verification	Verified?
Power Supply 1. Must supply 3.3V±0.1V DC	1. a. Plug the Power Supply module into the wall and b. Use a voltmeter to measure the output voltage for a continuous hour i. The output voltage must fall between 3.3V±0.1V	Y
RF Transceivers 1. RF transceivers must correctly receive more than 99% of wireless data sent	1. a. Set up the system normally b. Use the sniffer to broadcast 100 bits of data at 868MHz band using all channel from channel 0 to channel 31 c. Use an oscilloscope to monitor the output from the RF transceivers d. The output must output more than 99 bits of data sent by the sniffer correctly	N
2. Communicate with another transceiver 20 m ± 5 m away	2. a. Set up the system normally b. Use the transceiver to broadcast 100 bits of data at 868MHz band using all channel from channel 0 to channel 31 c. Place the sniffer 20 m ± 5 m away from the transceiver d. Use an oscilloscope to monitor the output from the RF transceivers e. At least 99 bits of data must be correct	Y
Microcontroller 1. Must be able to output data using SPI protocol correctly more than 99% of the time	1. a. Set up the system normally b. Connect the output of the microcontroller module to an oscilloscope c. Output a 100 bits of data from the microcontroller d. At least 99 bits of data displaying on the oscilloscope must match the data sent.	Y
2. Must parse data received from the SPI protocol and generate a response correctly 99% of the time	2. a. Set up the system normally b. Use the sniffer to broadcast spoofed data at 868MHz band at all channels from 0 to 31 c. Use an oscilloscope to monitor the output of the RF transceiver	Y

	d. Verify the SPI interface output from the RF transceiver is correct e. Use an oscilloscope to monitor the output of the microcontroller SPI interface f. The correct response must be seen on the oscilloscope g. Repeat a to k 100 times h. At least 99 times the test must pass	

Appendix B Software Flowchart

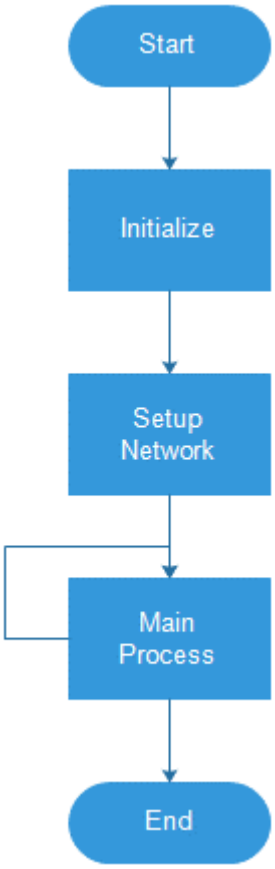


Figure 7 Main Flowchart

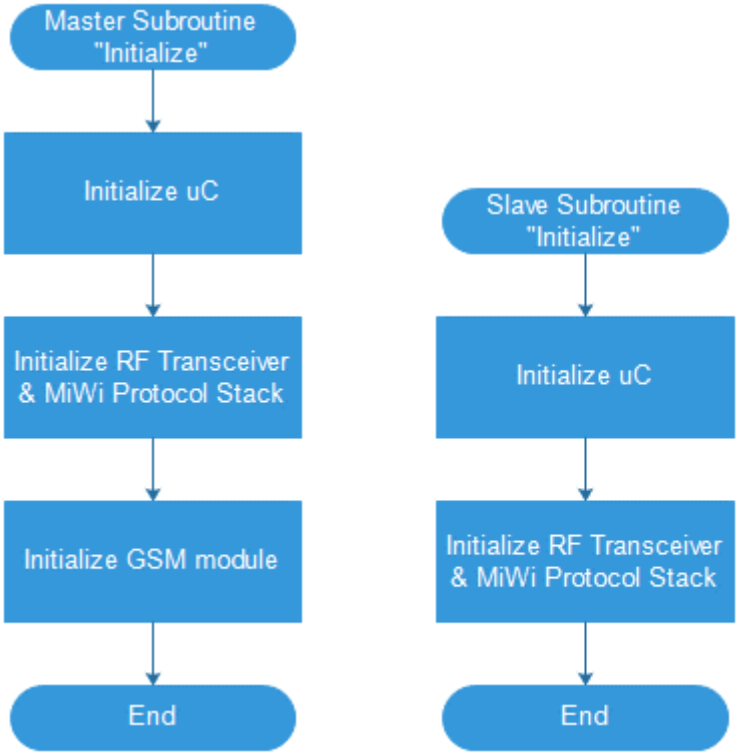


Figure 8 Master (Left) and Slave (Right) Initilize Flowchart

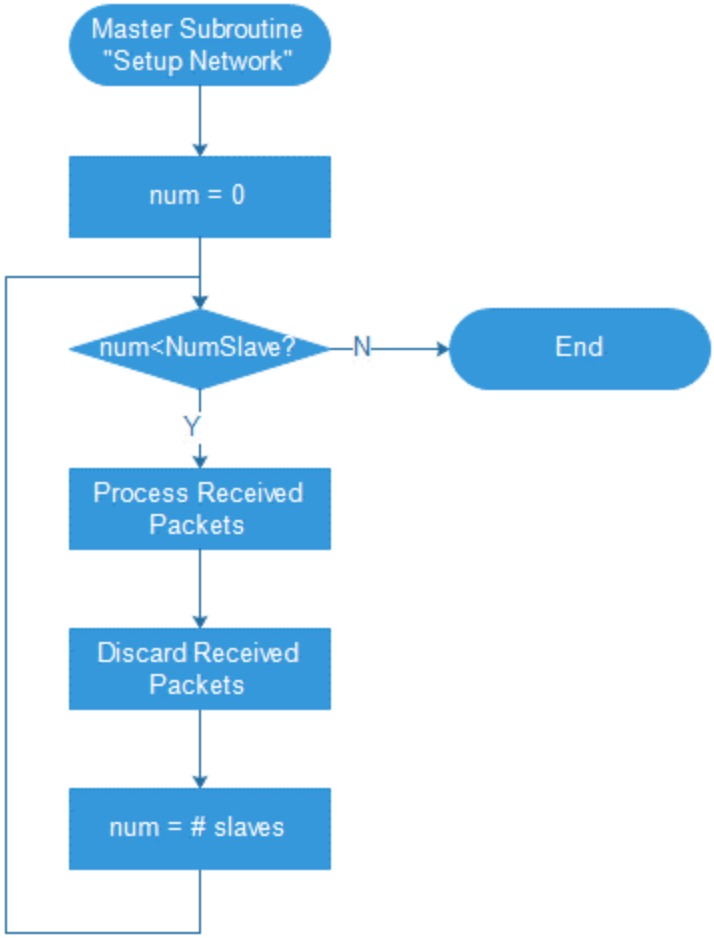


Figure 9 Master Setup Network Flowchart

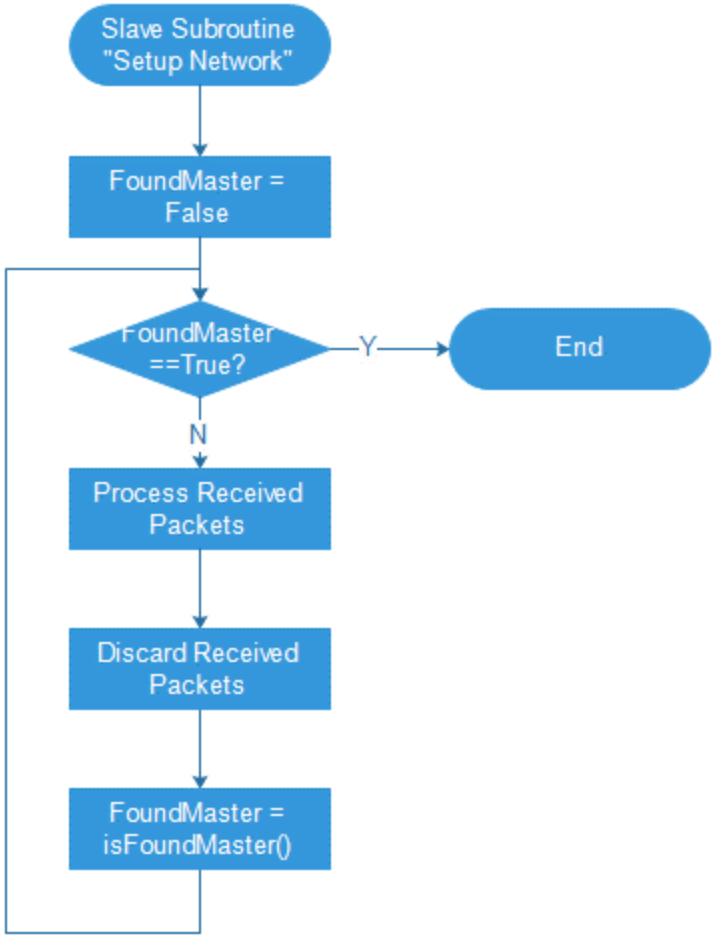


Figure 10 Slave Setup Network Flowchart

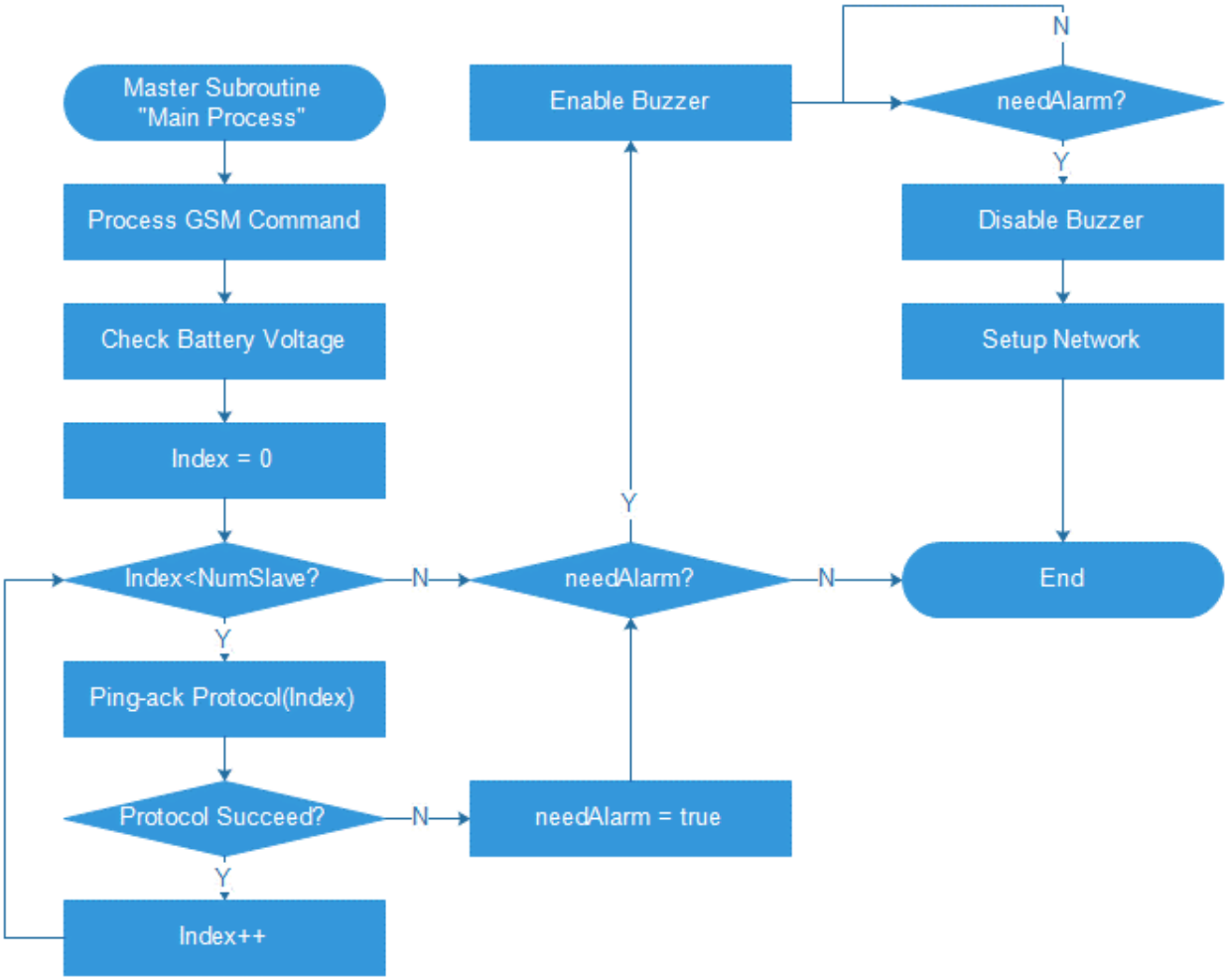


Figure 11 Master Main Process Flowchart

Appendix C Data Encryption Algorithm - TEA

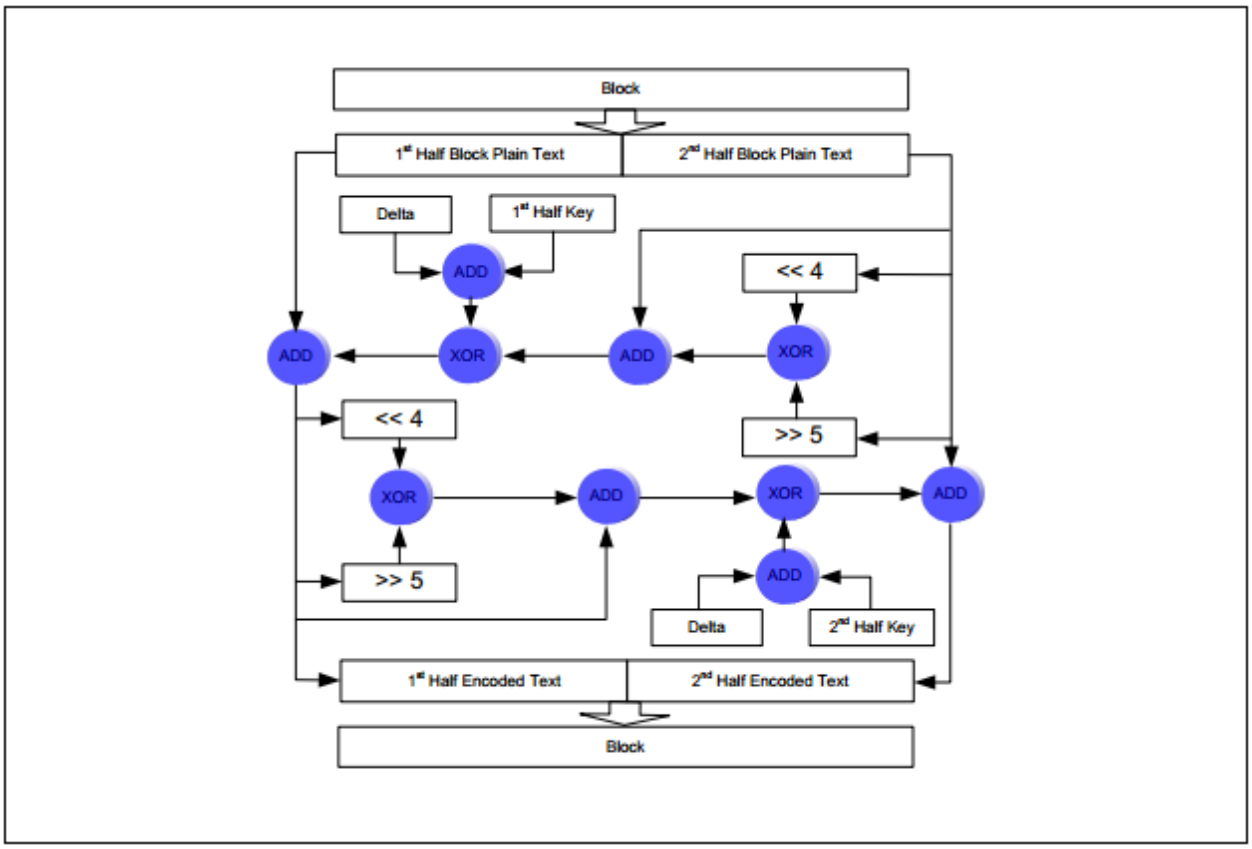


Figure 12 TEA Encryption Algorithm [3]

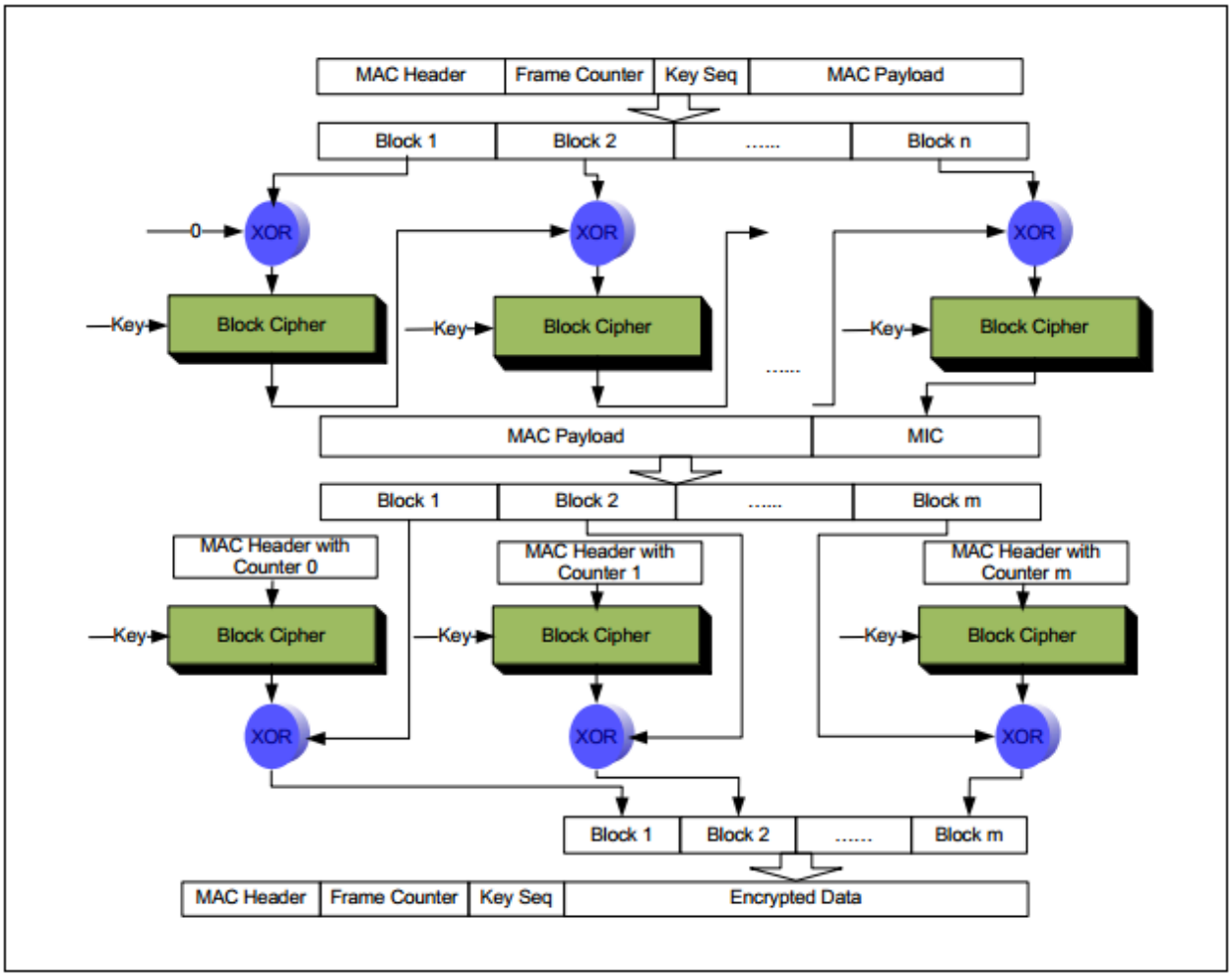


Figure 13 TEA in CBC Mode [3]

Appendix D Verification Tools

D.1 ZENA Wireless Adapter

ZENA Wireless Adapter is a network sniffer [4]. It comes in three models, which operate at 868MHz, 915MHz, and 2.4GHz. Since our system will be operating at 868MHz band, a ZENA Wireless Adapter for 868MHz band will be used. The sniffer listens passively to any packets on the 868MHz band and display the received packets in a human readable format on a computer with the help of a free software, Wireless Development Studio (WDS), developed by Microchip.

The adapter is also capable of sending out packets, meaning that the adapter can be configured to be one of the nodes in the network. Both of the adapter's functions can be used to verify the correctness of our system.

D.2 USB to Serial Converter

Since there is not a serial COM port on my computer, a USB to serial port converter has to be used, so that traffics on the UART interface can be monitored on the computer. The converter essentially contains a CP2102 chip, which does the conversion. A program called HyperTerminal also has to be used with the simulated serial port, in order to visualize the intercepted traffics.

Appendix E Mobile App User Interface

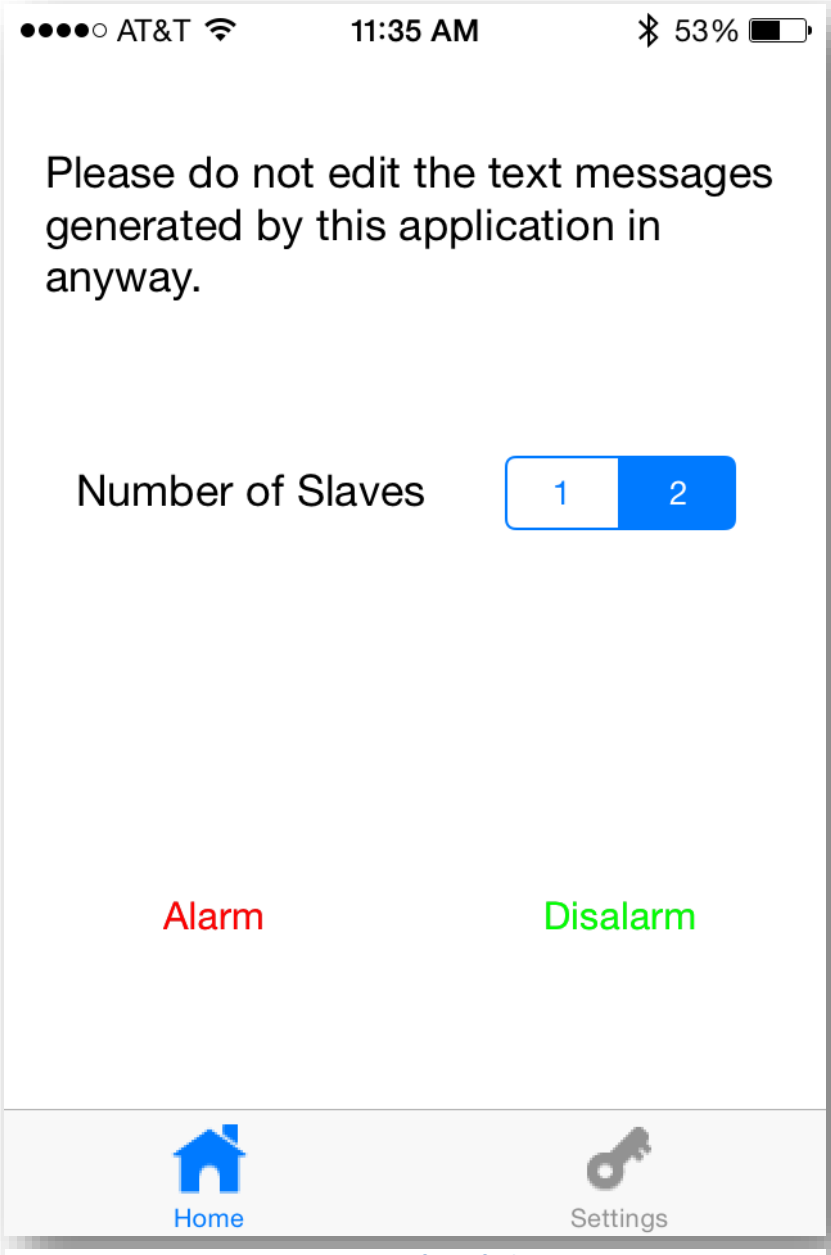


Figure 14 User Interface of iPhone App

Appendix F Test Results

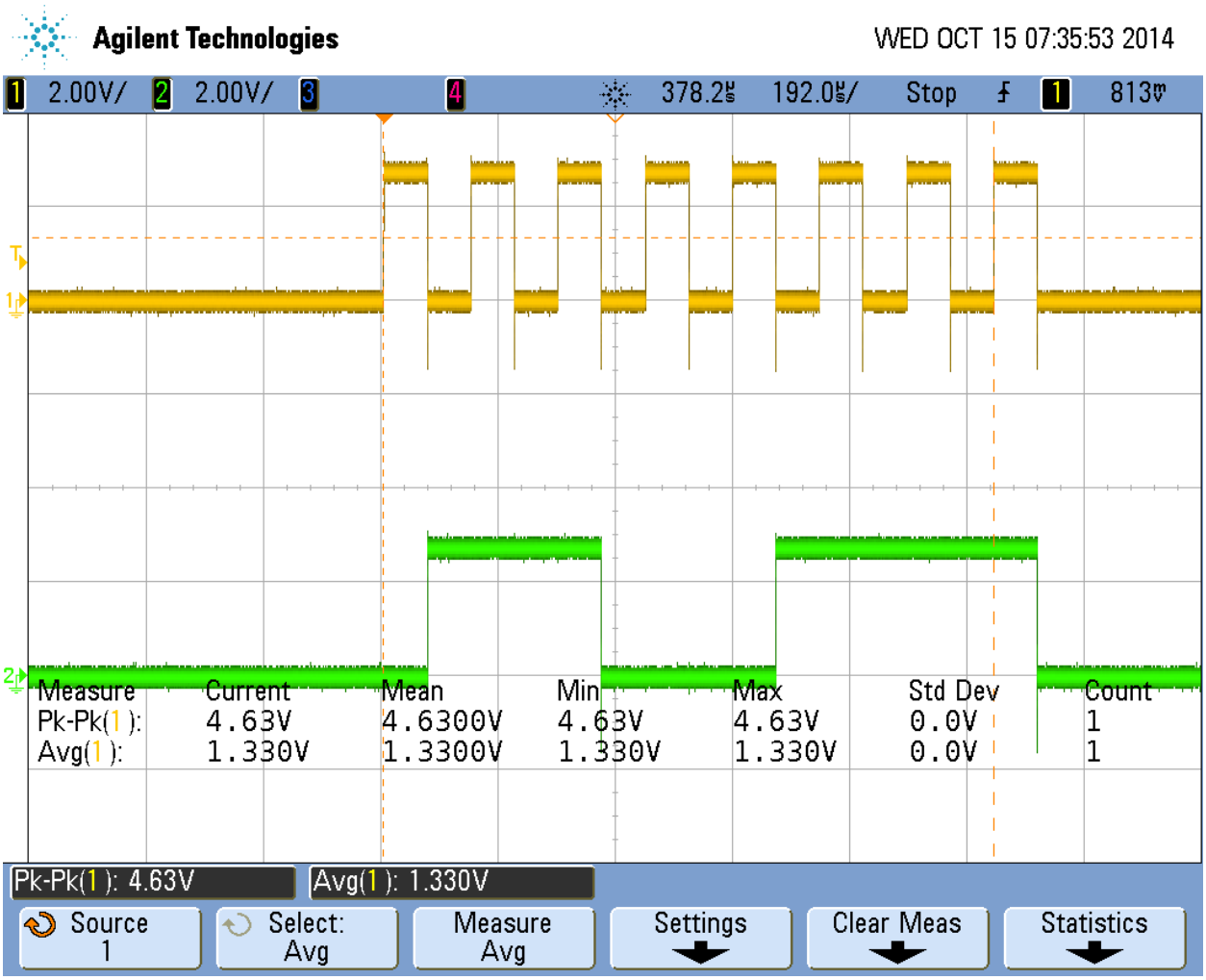


Figure 15 SPI Data Out

Frame No.	Time Stamp	RSSI	Source Addr.	Destination Ad...	Packet Info
1	+ 8704953 ...	57	0x11111111	0xffffffff	*MiWi P2P Command : P2P Connection Request*
2	+ 883616 us	61	0x33333333	0xffffffff	*MiWi P2P Command : P2P Connection Request*
3	+ 13443 us	54	0x11111111	0x33333333	*MiWi P2P Command : P2P Connection Response*
4	+ 10694 us	54	0x11111111	0xffffffff	*MiWi P2P Command : P2P Connection Request*
5	+ 1984077 ...	58	0x11111111	0xffffffff	*MiWi P2P Command : P2P Connection Request*
6	+ 1045574 ...	60	0x22222222	0xffffffff	*MiWi P2P Command : P2P Connection Request*
7	+ 13504 us	60	0x11111111	0x22222222	*MiWi P2P Command : P2P Connection Response*
8	+ 357911 us	62	0x11111111	0x33333333	*Data*
9	+ 11806 us	60	0x33333333	0x11111111	*Data*
10	+ 72471 us	62	0x11111111	0x22222222	*Data*
11	+ 11790 us	64	0x22222222	0x11111111	*Data*
12	+ 762878 us	54	0x11111111	0x33333333	*Data*
13	+ 11630 us	61	0x33333333	0x11111111	*Data*
14	+ 72563 us	54	0x11111111	0x22222222	*Data*
15	+ 11741 us	61	0x22222222	0x11111111	*Data*
16	+ 762914 us	56	0x11111111	0x33333333	*Data*
17	+ 11729 us	61	0x33333333	0x11111111	*Data*

Figure 16 Star Topology & Ping-ack Protocol

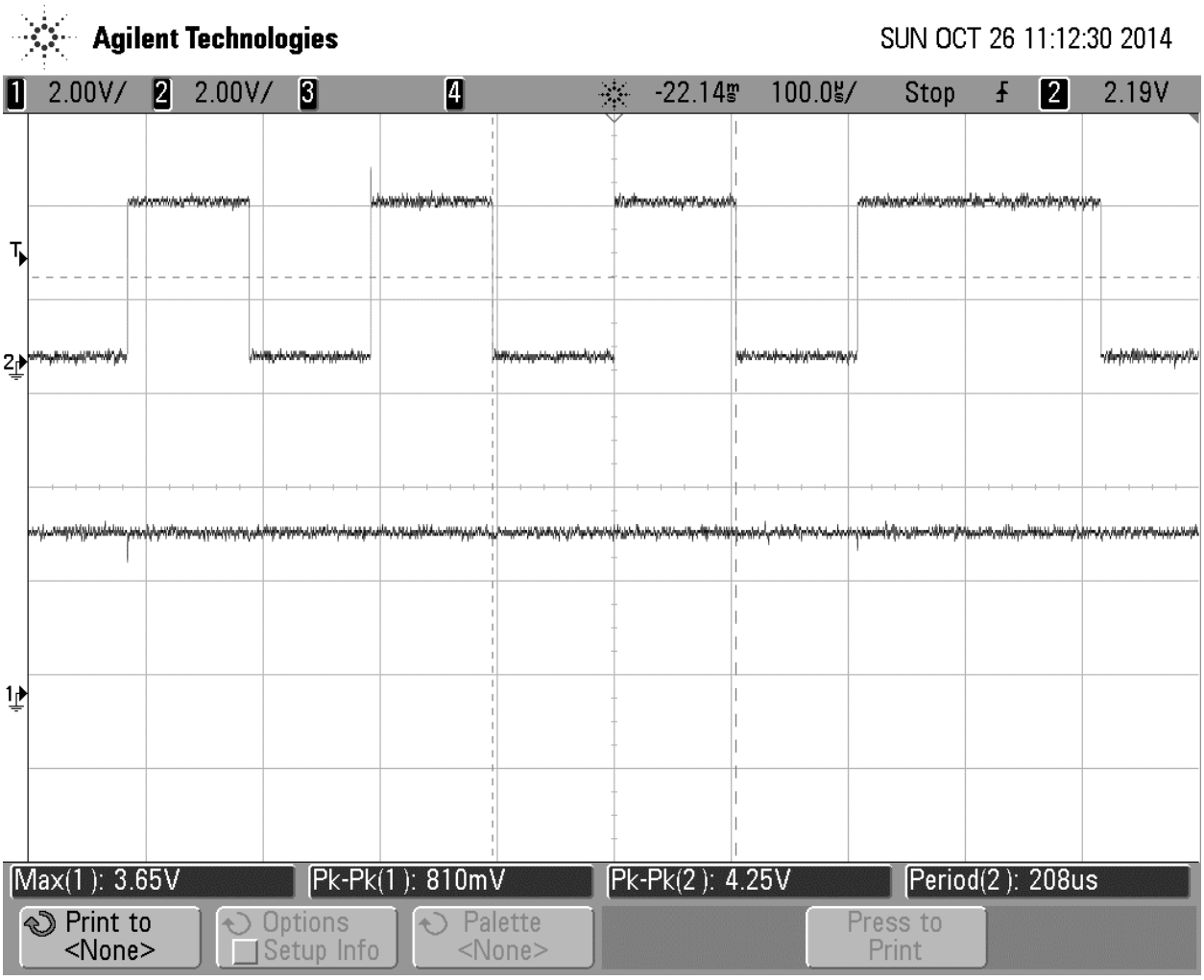


Figure 17 UART Data Rate

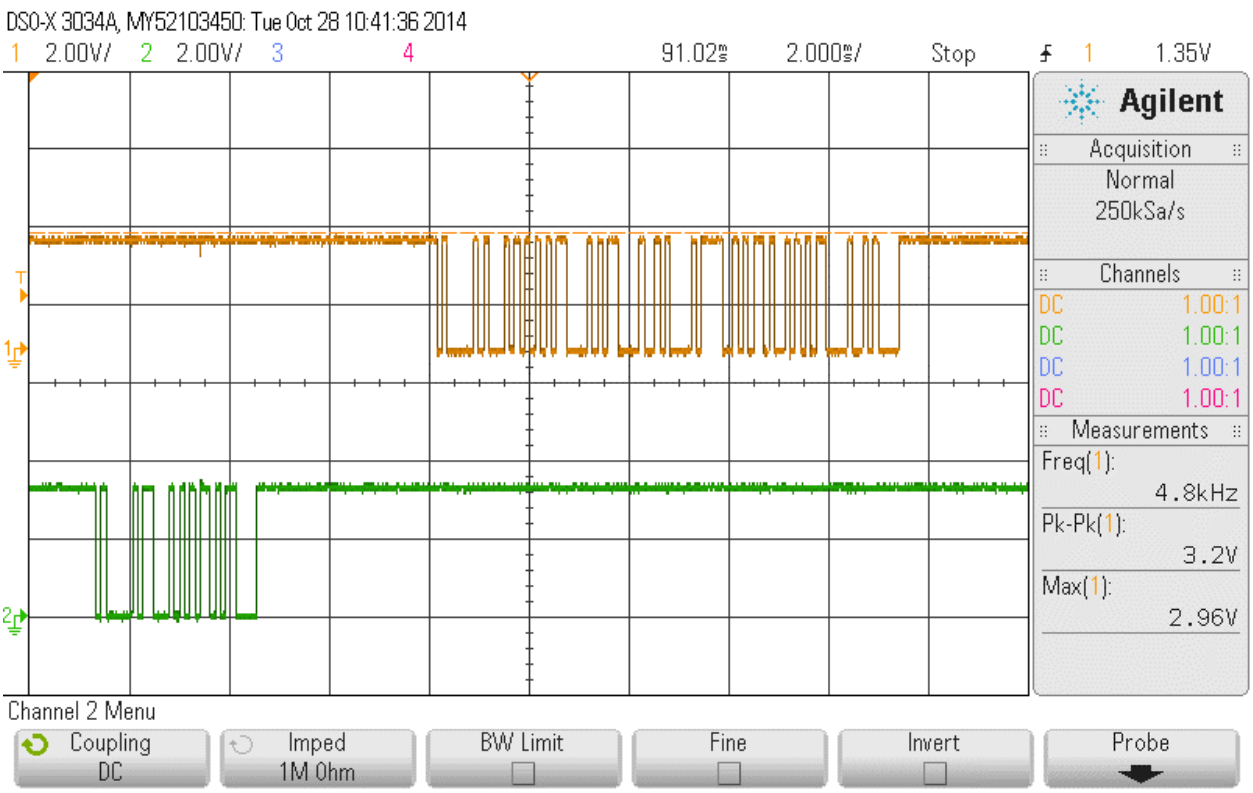


Figure 18 UART Working

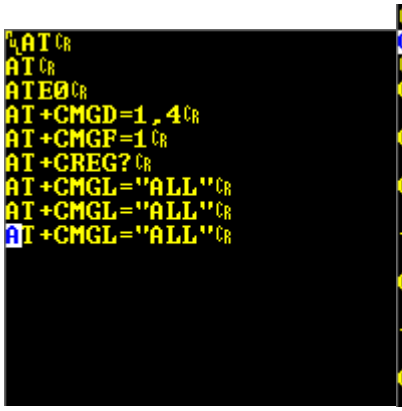


Figure 19 Command for GSM

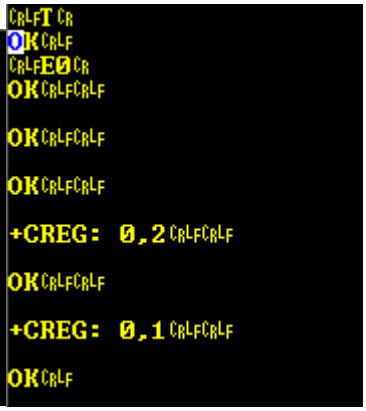


Figure 20 Responses from GSM

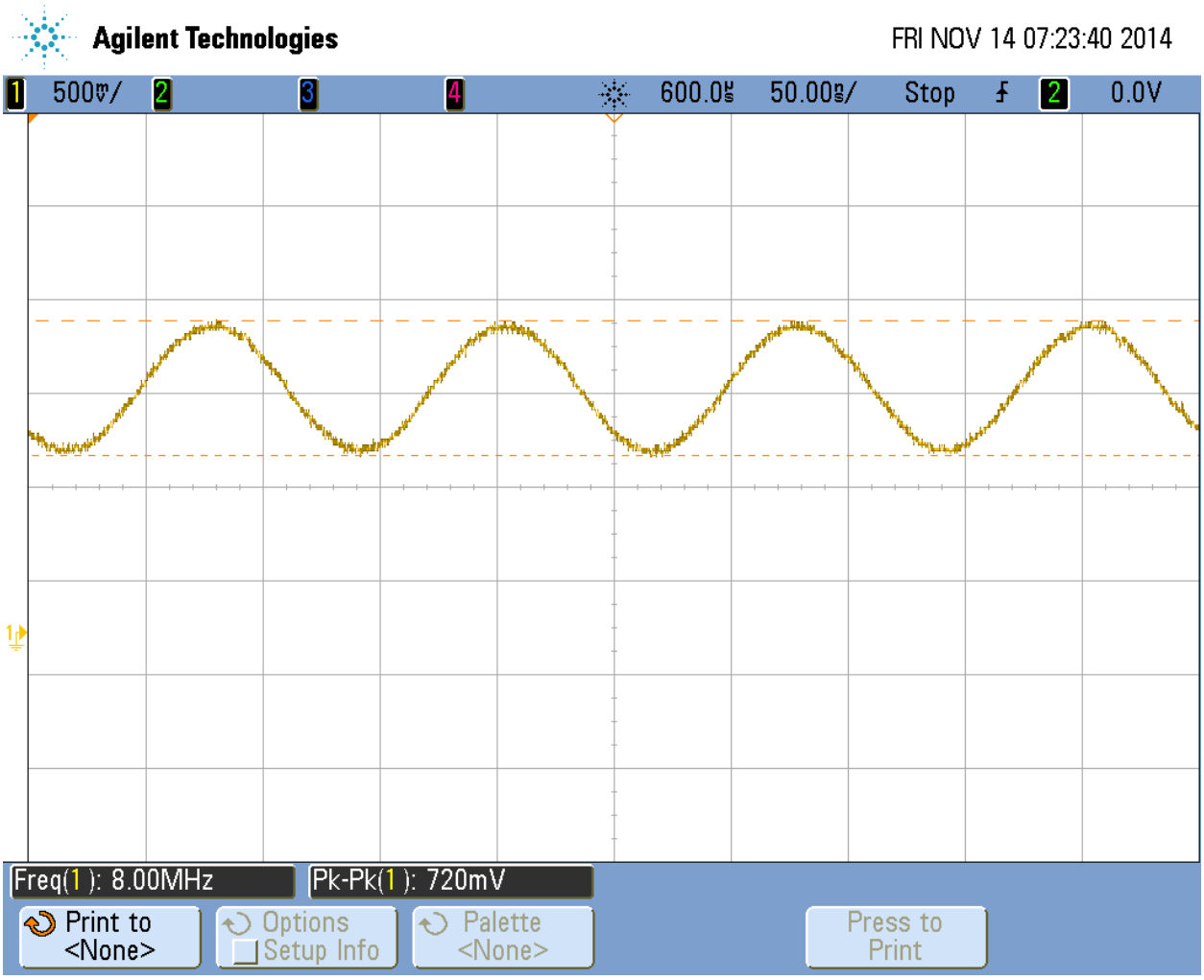


Figure 21 8MHz Crystal

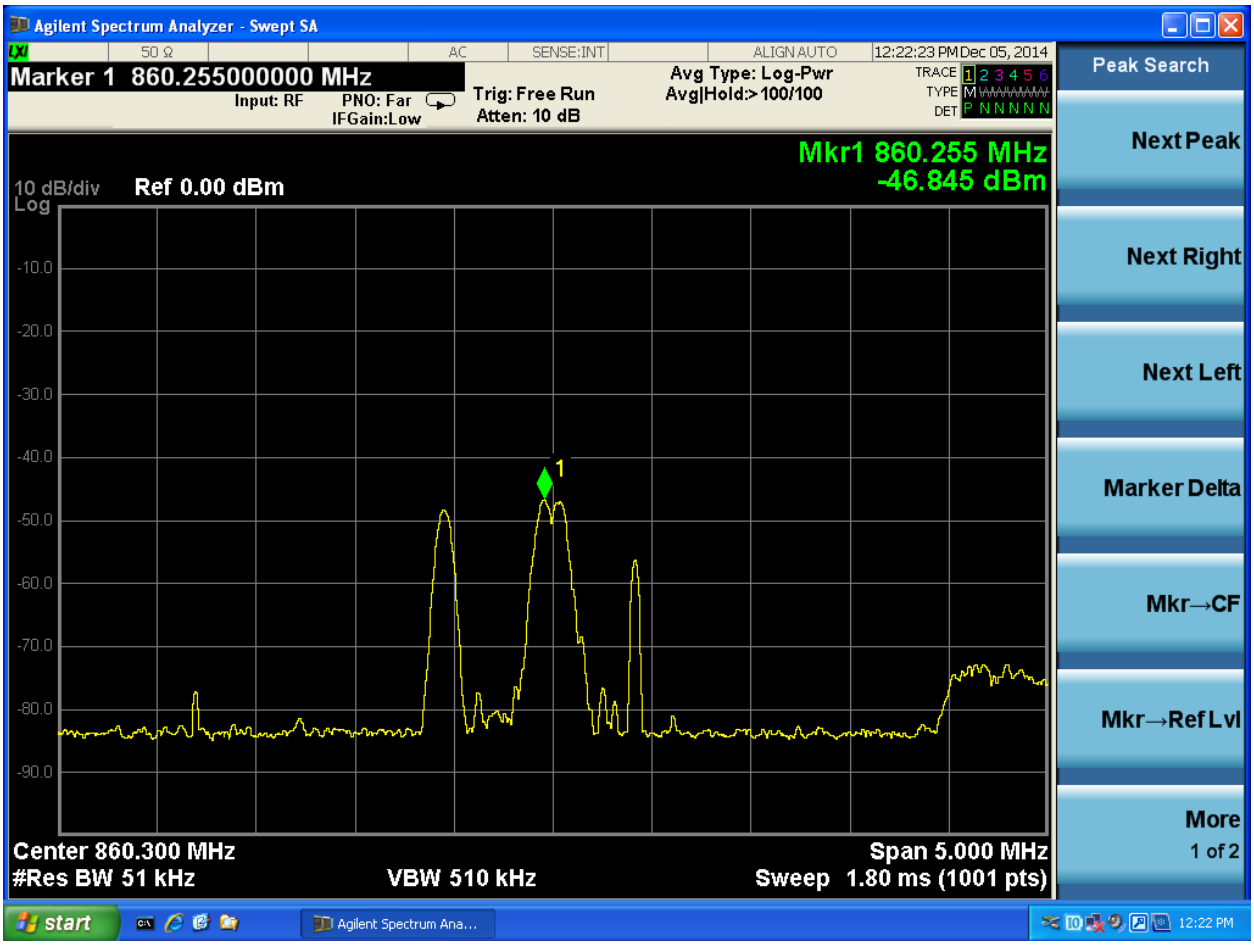


Figure 22 Matched Signal Strength

Appendix G PCB Diagrams and Layouts

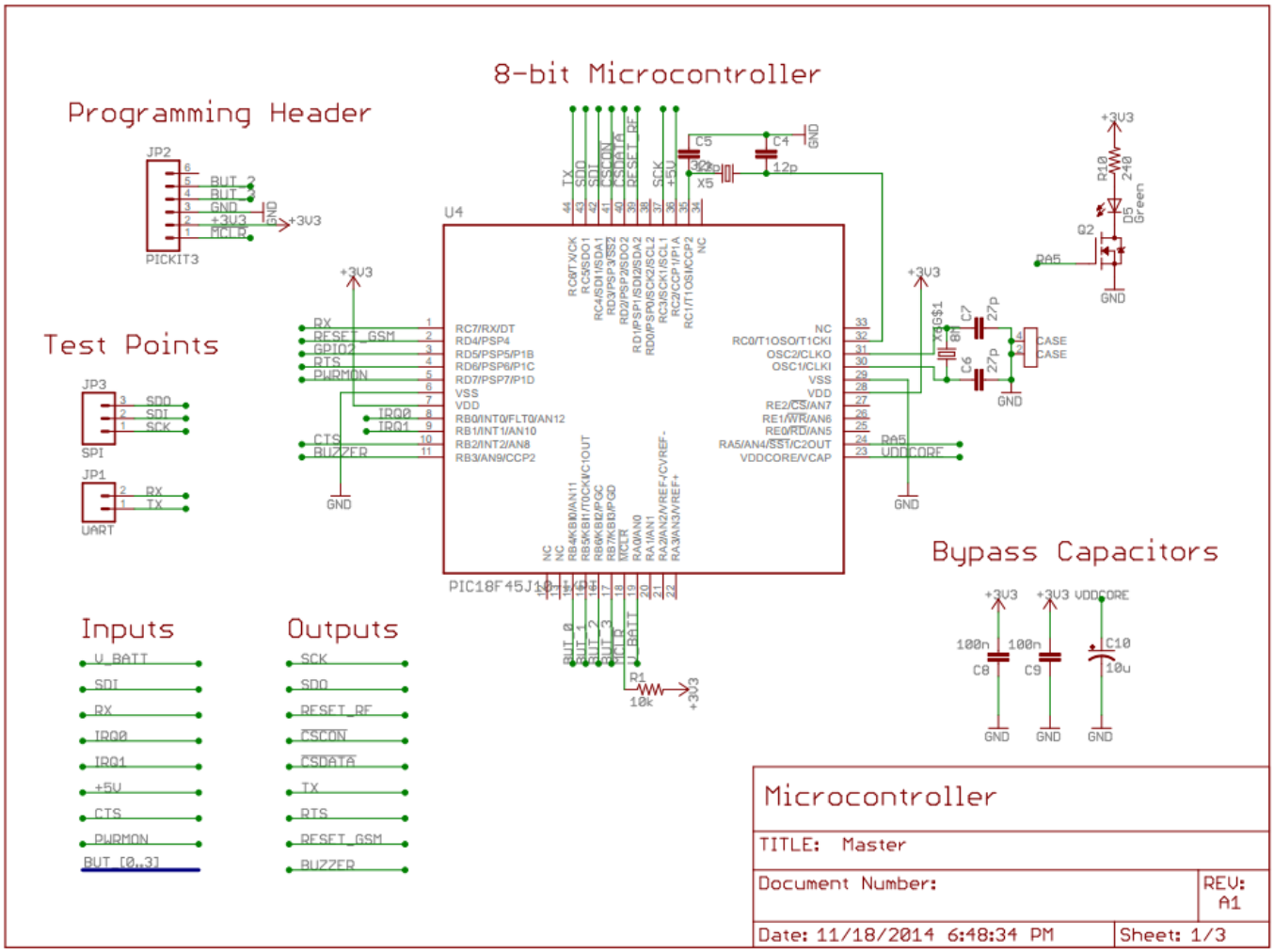


Figure 23 Master Circuit Diagram Page 1

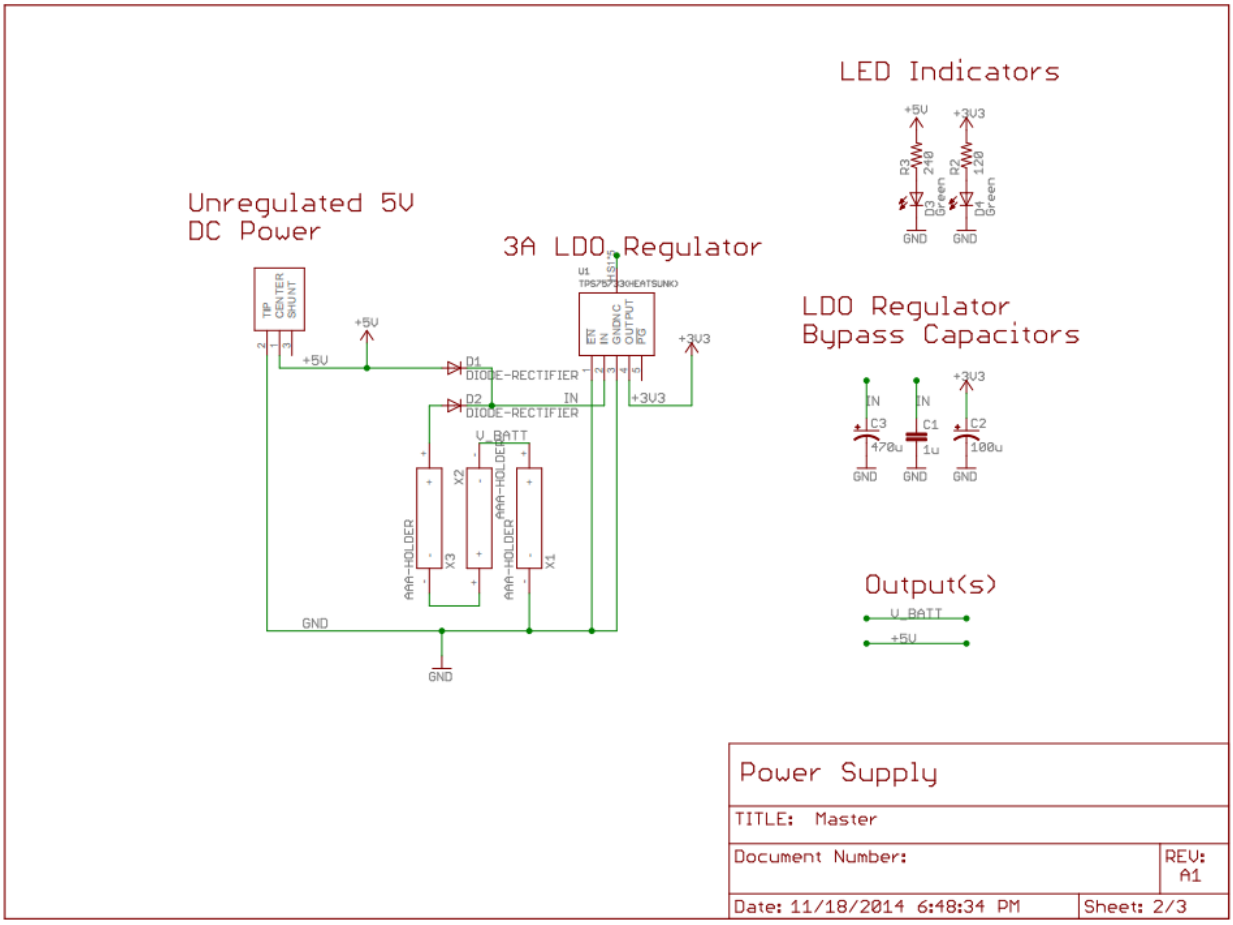


Figure 24 Master Circuit Diagram Page 2

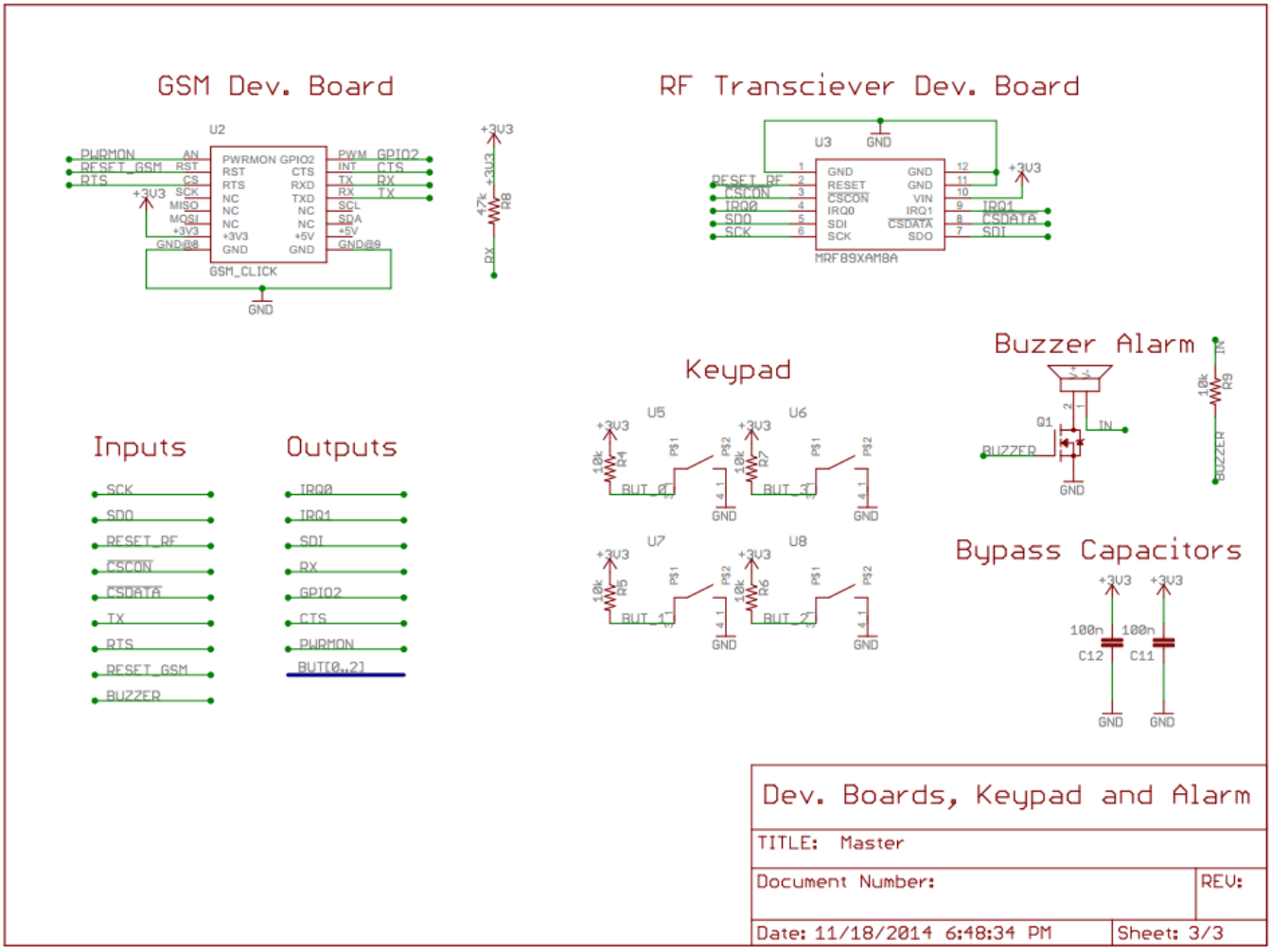


Figure 25 Master Circuit Diagram Page 3

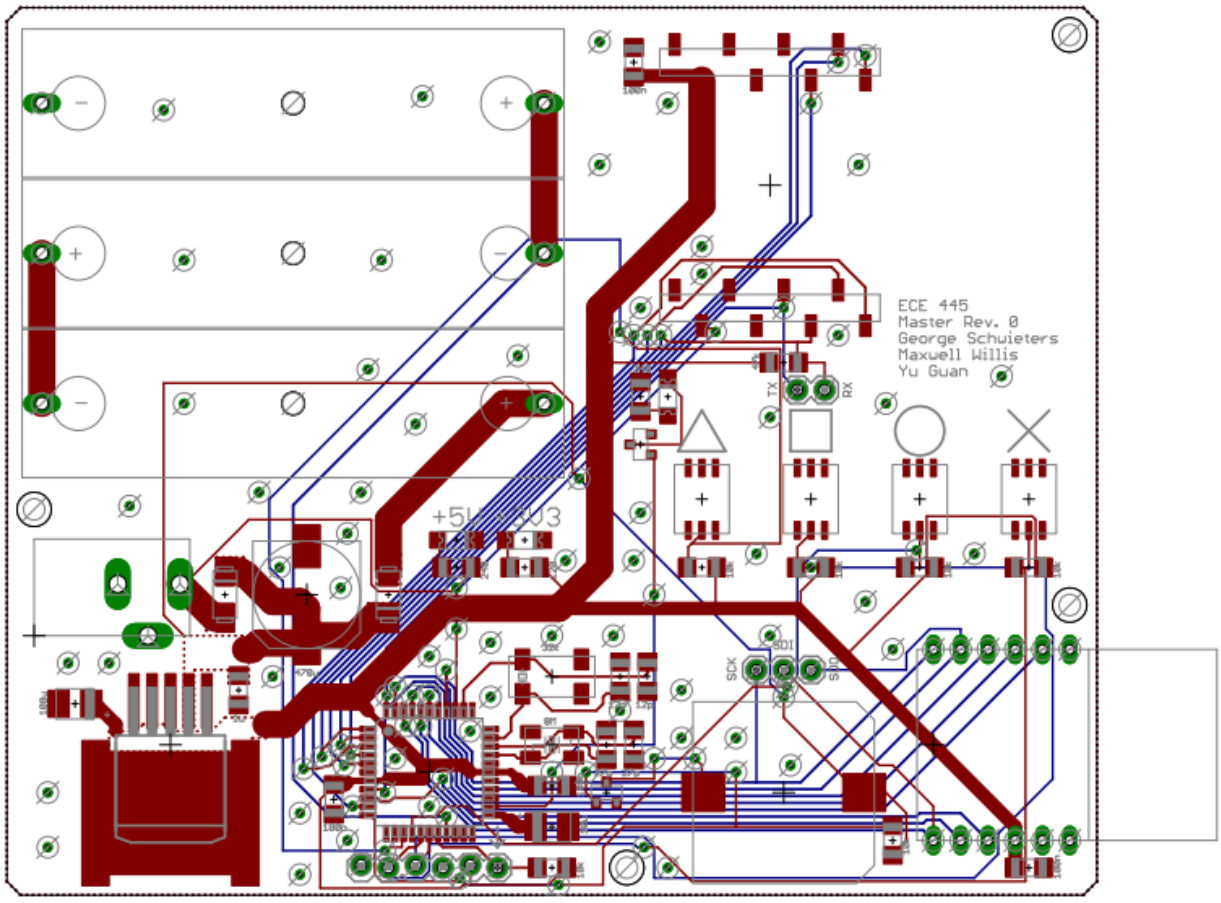


Figure 26 Master Layout All Layers

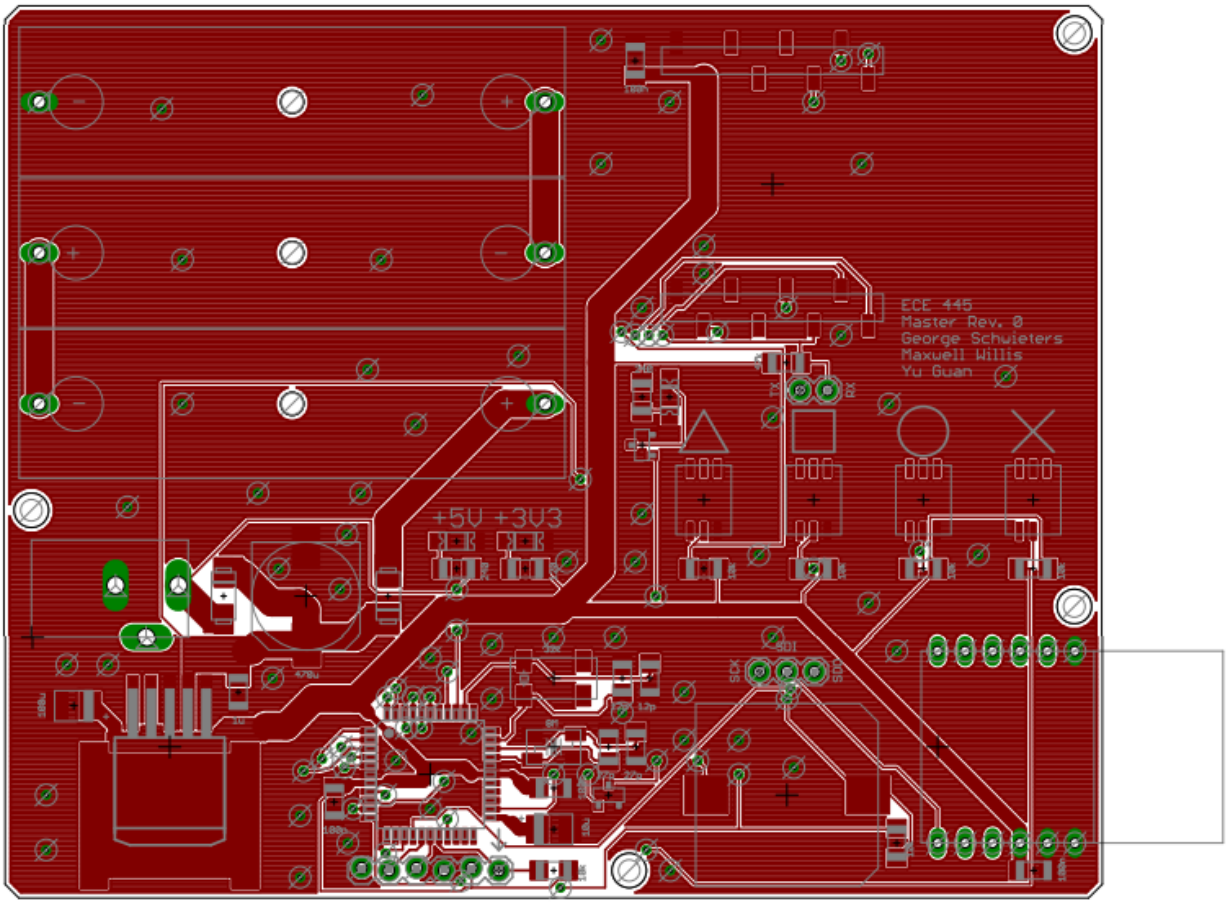


Figure 27 Master Layout Top Layers

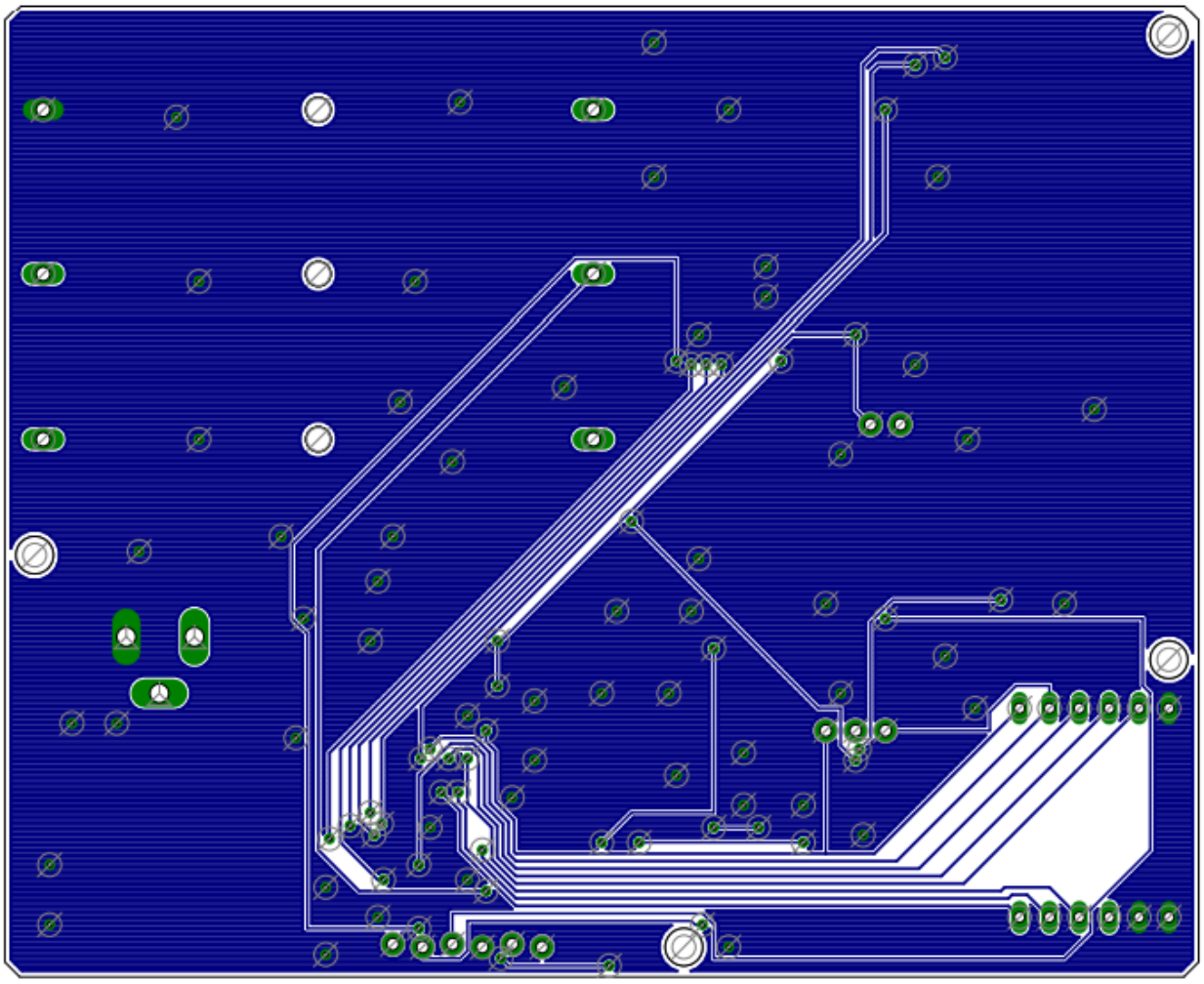


Figure 28 Master Layout Bottom Layers

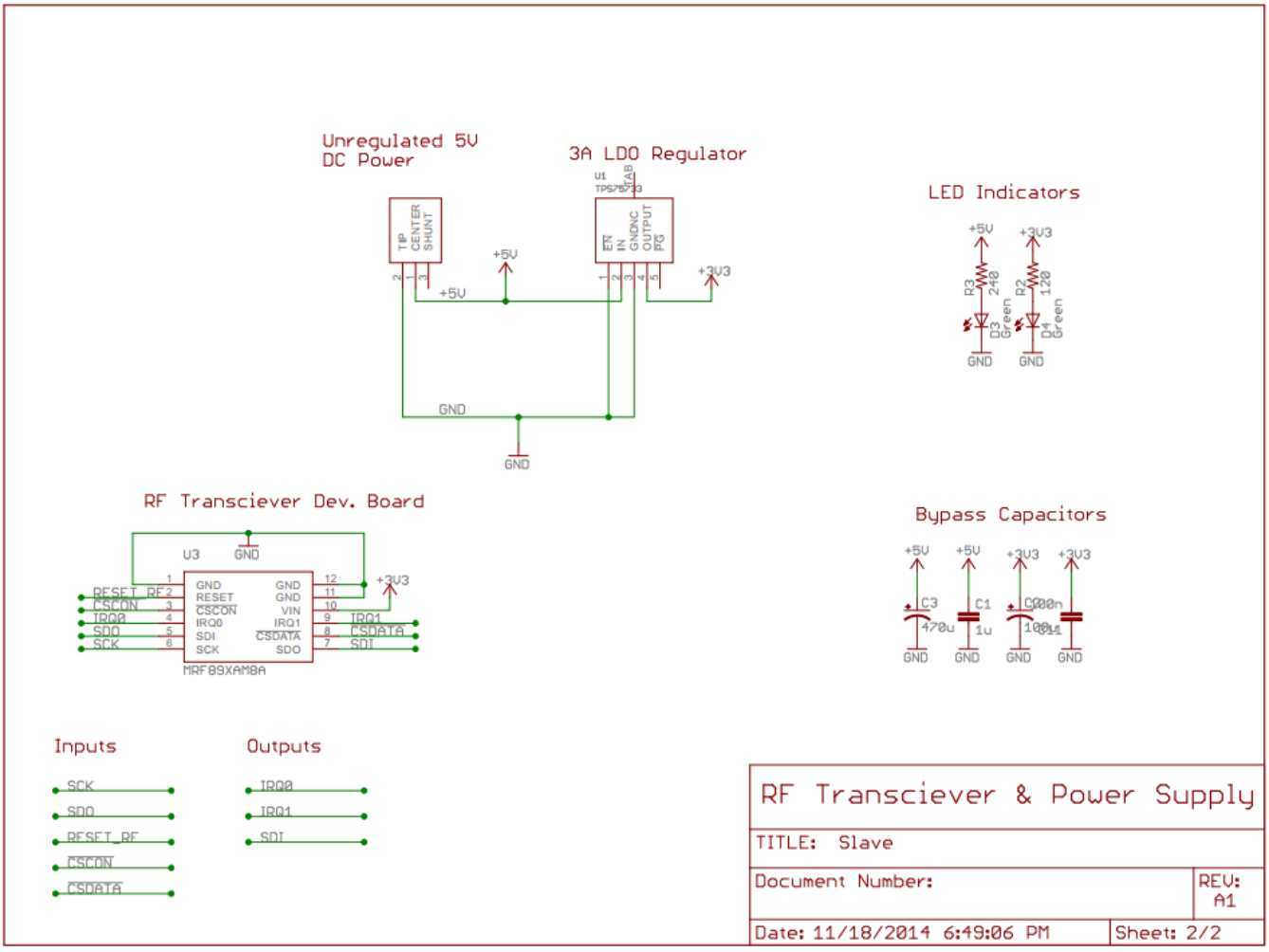


Figure 29 Slave Circuit Diagram Page 1

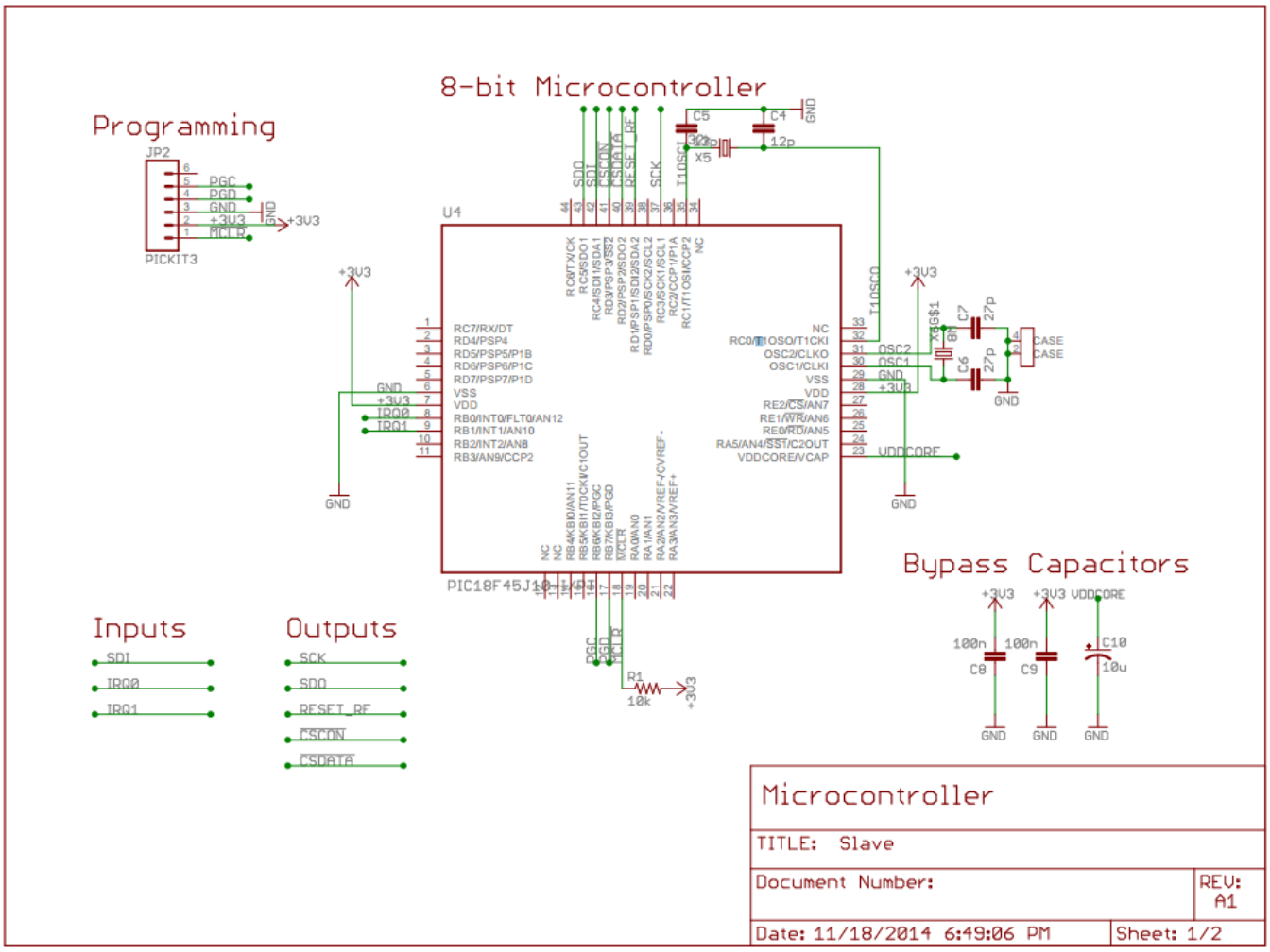


Figure 30 Slave Circuit Diagram Page 2

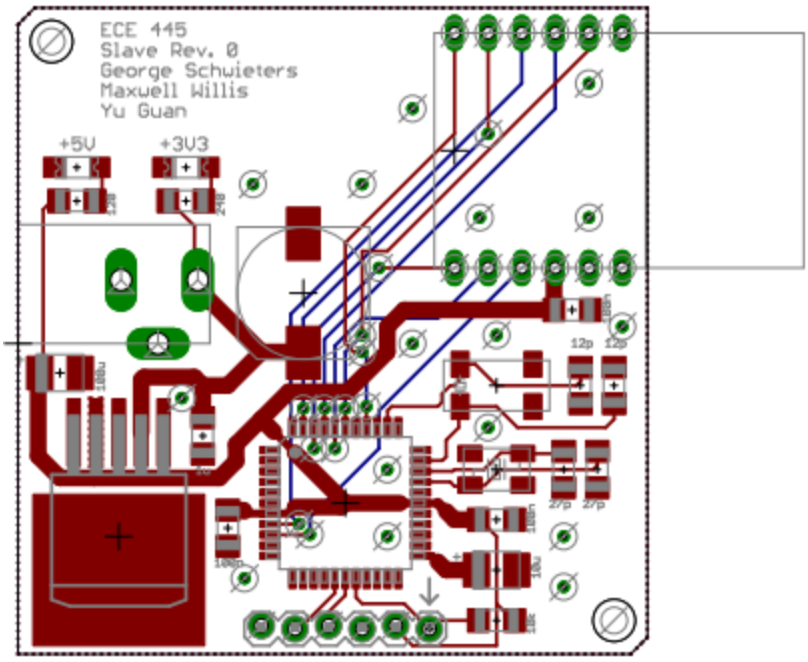


Figure 31 Slave Layout All Layers

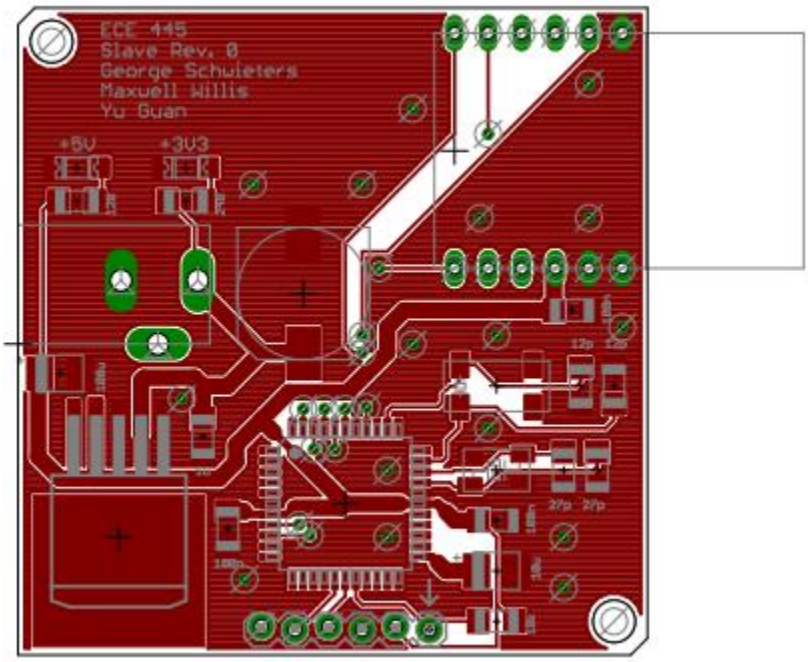


Figure 32 Slave Layout Top Layers

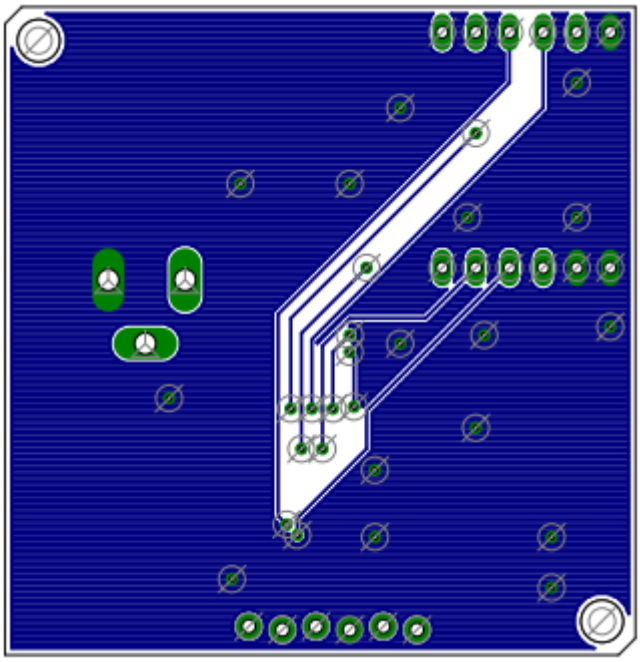


Figure 33 Slave Layout Bottom Layers

Appendix H Cost Table

	Package	Unit Cost	Qty	Vendor	Description
PIC18 & Supporting Components					
Logic					
PIC18F45J10-I/PT	TQFP-44	$2.08	1	Allied Electronics	8-bit microcontroller
Discrete					
LTST-C150GKT	1206	$0.37	2	Digi-Key	green 2.1V 10mA 6mcd LED
Passive					
ABS25-32.768KHZ-T	SMD-4	$0.71	1	Digi-Key	32.768Khz 12.5pF 20ppm crystal
ABM3B-8.000MHZ-B2-T	SMD-4	$1.14	1	Mouser	8Mhz 18pF 20ppm crystal
C1206C120J5GACTU	1206	$0.02	2	Allied Electronics	12pF 50V COG ceramic capacitor
C1206C270J5GACTU	1206	$0.02	2	Allied Electronics	27pF 50V COG ceramic capacitor
C1206C104K5RACTU	1206	$0.07	2	Allied Electronics	100nF 50V X7R ceramic capacitor
293D106X9016B2TE3	3528	$0.30	1	Allied Electronics	10uF 16V 2Ohm tantalum capacitor
PCF1A471MCL1GS	SMD-2	$2.01	1	Digi-Key	470uF 10V 16mOhm electrolytic capacitor
RC1206JR-07120RL	1206	$0.10	1	Digi-Key	120Ohm 1/4W 1% resistor
ERJ-8ENF6040V	1206	$0.10	1	Digi-Key	240Ohm 1/4W 1% resistor
CRCW120610K0FKEA	1206	$0.10	1	Allied Electronics	10kOhm 1/4W 1% resistor
Summary					
PIC18 w/ SUPPORTING TOTAL		*$7.32*	*16*		
Master					
Logic					
PIC18 & Supporting Components	[redacted]	$7.32	1	Various	PIC18 Microcontroller and Supporting Components
GSM Click	Through Hole	$49.00	1	MikroElectronica	GSM Dev. Board
MRF89XAM8A	SMD-12	$9.54	1	Digi-Key	RF Transciever Dev. Board
Power					
EPSA050250U-P5P-EJ	N/A	$12.30	1	Digi-Key	5V 3A Wall Adapter (DC jack, positive center)
TPS75733KTTT	DDPAK-5	$7.78	1	Digi-Key	3.3V 3A LDO voltage regulator
Discrete					
LTST-C150GKT	1206	$0.37	1	Digi-Key	green 2.1V 10mA 6mcd LED
2N7002-7-F	SOT23	$0.15	2	Digi-Key	115mA 60V N channel MOSFET
SK34A-LTP	SMA	$0.57	2	Digi-Key	3A 500mV schottky diode
Passive					
RC1206JR-07120RL	1206	$0.10	1	Digi-Key	120Ohm 1/4W 1% resistor
C1206C104K5RACTU	1206	$0.07	2	Allied Electronics	100nF 50V X7R ceramic capacitor
C1206C105K5RACTU	1206	$0.10	1	Allied Electronics	1uF 50V X7R ceramic capacitor
293D107X96R3B2TE3	3528	$0.91	1	Digi-key	100uF tantalum capacitor
CRCW120610K0FKEA	1206	$0.10	4	Allied Electronics	10kOhm 1/4W 1% resistor
Other					
CMI-1240-SMT	SMD-2	$4.81	1	Digi-Key	12V 4kHz buzzer
1.14002.1010000	SMD-6	$2.20	4	Digi-Key	SPST 100mA 35V pushbutton

Figure 34 Bill of Materials Page 1

	Package	Unit Cost	Qty	Vendor	Description
NPTC081KFXC-RC	Through Hole	$1.50	2	Digi-Key	8 pin female header
68000-408HLF	Through Hole	$0.29	2	Digi-Key	8 pin male header
BCAAAPC	Through Hole	$1.01	3	Digi-Key	AAA battery holder
18742	Through Hole	$0.95	1	SparkFun	DC power jack connector
MN2400	N/A	$0.59	3	Amazon	Duracell Coppertop AAA battery
573300D00010G	SMD	$0.84	1	Digi-Key	18 *C/W DDPAK heatsink
Summary					
MASTER TOTAL		*$113.17*	*51*		
Slave					
Logic					
PIC18 & Supporting Components	[redacted]	$7.32	1	Various	PIC18 Microcontroller and Supporting Components
MRF89XAM8A	SMD-12	$9.54	1	Digi-Key	RF Transciever Dev. Board
Power					
EPSA050250U-P5P-EJ	N/A	$12.30	1	Digi-Key	5V 3A Wall Adapter (DC jack, positive center)
TPS75733KTTT	DDPAK-5	$7.78	1	Digi-Key	3.3V 3A LDO voltage regulator
Passive					
C1206C104K5RACTU	1206	$0.07	1	Allied Electronics	100nF 50V X7R ceramic capacitor
C1206C105K5RACTU	1206	$0.09	1	Allied Electronics	1uF 50V X7R ceramic capacitor
293D107X96R3B2TE3	3528	$0.91	1	Digi-key	100uF tantalum capacitor
Other					
18742	Through Hole	$0.95	1	SparkFun	DC power jack connector
Summary					
SLAVE TOTAL		*$38.96*	*23*		
Total					
Section	Unit Cost	Qty			
PCB Manufacturing	$33.00	3			
Master Total	$113.17	1			
Slave Total	$38.96	2			
GRAND TOTAL	$290.08				

Figure 35 Bill of Materials Page 2