Wireless IntraNetwork

Team 1 — Daniel Gardner and Jeeth Suresh
ECE 445 Project Proposal — Fall 2016
TA: Jamie Norton

1 Introduction

1.1 Objective

The internet is such an important part of modern life that the UN has defined it as a basic human right. Unfortunately, 60% of the human race (over four billion people) still lack any kind of connection to this invaluable service. There is a giant gap in internet availability between the developed and developing world today. In regions such as Sub-Saharan Africa, less than 0.5% of people[1] have a fixed internet broadband subscription. This leads to social, educational, and economic isolation. LTE and HSPA coverage, the two leading standards of mobile connectivity, have a combined coverage of just 25% of the region[2]. In comparison, in the US a phone will spend over 85% of its time covered by an LTE signal[3] and 70% of adults have an active broadband subscription[4]. A contributing factor to this massive difference in connectivity may be that sub-Saharan Africa is significantly less urbanized than the US - 64.2% of residents in the United States live in an urban environment versus 10.6% in Zimbabwe and 2.8% in Uganda[5]. Studies show that a 10% increase in internet access in a developing country brings a 1.7% increase in exports and 1.1% increase in imports [6]. Without reliable access to the wealth of educational, medical, and economic resources provided by the internet, Wi-fi enabled devices donated to villages in the developing world by organizations such as OLPC (One Laptop Per Child) will never achieve their full potential.

Our goal is to bring the internet to the developing world using an entirely new form of infrastructure. Instead of installing miles of fiber optic cables, our 'infrastructure' is almost entirely wireless. We will use a large number of solar-powered nodes to build a mesh network capable of transmitting data throughout a community, creating an intranet. These nodes will use Wi-fi so any device (whether it's been donated or purchased by a villager) can connect to the intranet and will adapt to the failures of other nodes using a reactive routing protocol.

1.2 Background

Efforts by Facebook, SpaceX, and Google attempt to solve the internet problem through low-flying satellites or drones, which suffer the same throughput bottlenecks as traditional satellite communication [7]. A mesh network that is easily-installed and expanded, while existing independently of expensive global connections, is the solution to connect remote areas of the world. Other attempts have been made to connect the world with remote, portable mesh networking [8]. Unfortunately, these have failed in the long term due to costs of over $200/node.

Our nodes must be as affordable as possible, to ensure that they can reasonably be purchased with the disposable income a rural villager might earn. A subsistence farmer in Nepal, for example, has a disposable income of about $5 per year [9]. We also plan to partner with NGOs to provide a subsidized distribution program so the node is cheaper (or even free) for the customer.

1.3 High-Level Requirements

- Nodes must be able to connect to each other automatically, allowing data stored on any node in the network to be available from any access point.
- Nodes must be able to operate indefinitely on solar power.
- Nodes must be as low-cost as possible, ideally under $20.

2 Design

Nodes require three sections for successful operation: a power supply, a control unit, and a WiFi module. The power supply ensures that the system can be powered continuously all day and night with the proper 3.3V. The control unit contains up to 16GB of storage for educational materials and other resources, as well as a microcontroller to handle this data. Lastly, a WiFi module connects this control unit to a standard IEEE 802.11b/g/n WiFi network. Each node will need to cover an area approximately 600-800ft in every direction with 4MB/s access. Nodes will also store 16GB of data for access by other users.

A central server is necessary for an optimized network, but its design is outside the scope of this class.

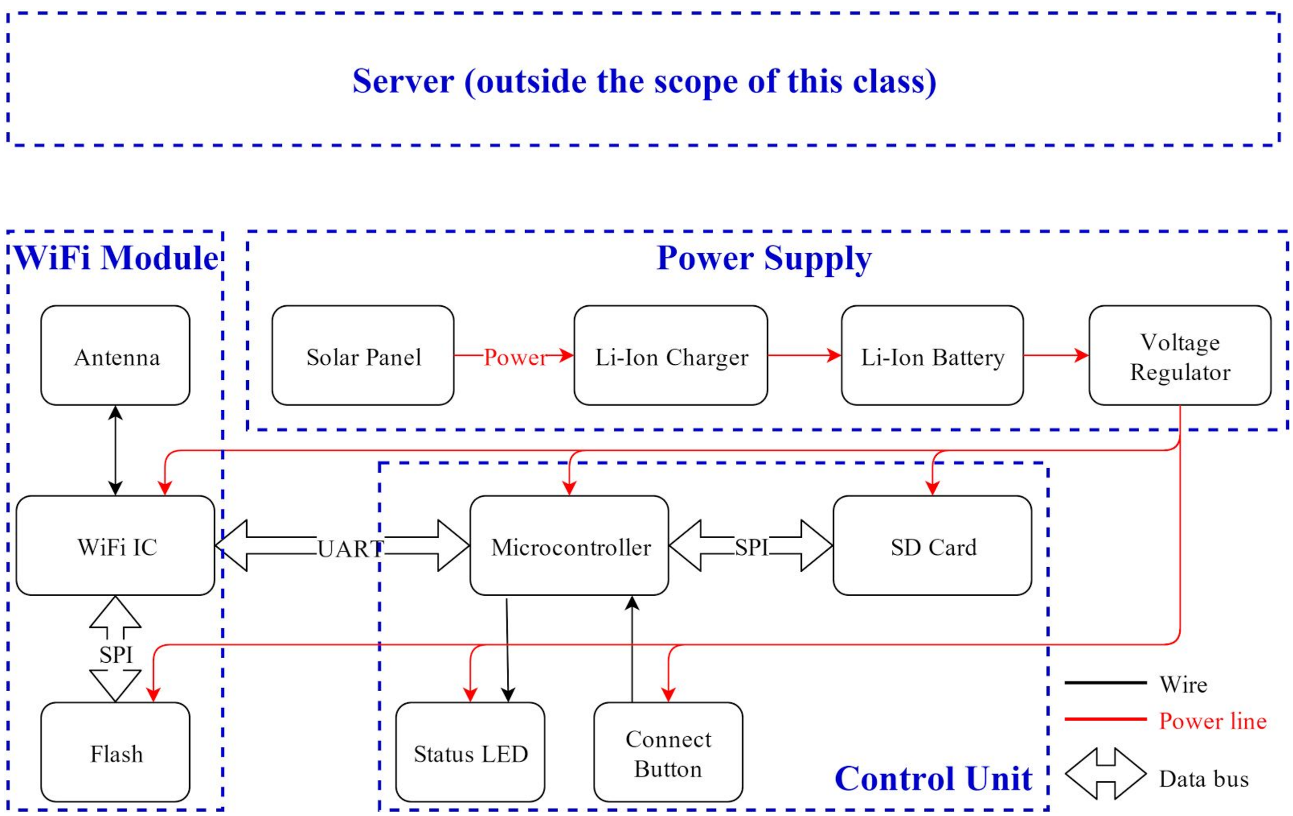

Figure 1. Block Diagram

2.1 Power Supply

A power supply is required to keep the communication network up continually. Power from a solar panel will charge a battery, which is then regulated to 3.3V for the rest of the system.

2.1.1 Solar Panel

Nodes will be powered by a solar panel. These will provide the charging IC with enough voltage to charge the battery, and enough power to keep the node continuously powered off of 10-12 hours of sunlight each day.

Requirement: Must provide >300mA between 4.45V-6.45V (the input voltage range for the Li-ion charger) in full sunlight

2.1.2 Li-ion charger

The node will charge the li-ion battery through a charging IC. This chip will charge the battery and be able to (thermally and electrically) charge the battery fully in only 10-12 hours. A li-ion charging cycle consists of constant-current to a specified voltage, followed by constant-voltage “float” charging to 4.2V. This second stage relies on the internal resistance of the battery to regulate current.

Requirement: Must charge the Li-ion battery to 4.16-4.23V with a continuous >300mA charge current, from a 4.4-7.0V source, and stay below 125°C (the maximum operating temperature).

2.1.3 Li-ion battery

The lithium-ion battery must be able to keep the circuit continuously powered, even at night with no power supplied by the solar panel.

Requirement: The battery must be able to store enough charge to provide at least 150mA at 3.7-4.2V for 14 hours with no sunlight.

2.1.4 Voltage regulator

This integrated circuit supplies the required 3.3V to the node system. This chip must be able to handle the peak input from the battery (4.2V) at the peak current draw (300mA).

Requirement 1: The voltage regulator must provide 3.3V +/- 5% from a 3.7-4.2V source.
Requirement 2: Must maintain thermal stability below 125°C at a peak current draw of 250mA.

2.2 Control Unit

A control unit manages the flash storage and prepares data to be sent over UART (Universal Asynchronous Receiver/Transmitter) to the WiFi module. A microcontroller controls an SD card and provides a small user interface with an LED and buttons.

2.2.1 Microcontroller

The microcontroller, chosen to be a PIC32, handles memory allocation for the cache. It communicates with the WiFi chip via UART and reads the SD card cache through SPI (Serial Peripheral Interface).

Requirement 1: The microcontroller must be able to communicate over UART and SPI simultaneously at speeds greater than 4.5Mbps (each).
Requirement 2: Must sink or source 10mA on each of two GPIOs at 3.3V +/- 5%.

2.2.2 SD card

The microSD card within each node will provide the cache from which a node will be able to operate. In the future, we plan to replace this with SMT flash storage.

Requirement: The SD card must provide both read and write speeds above 4.5Mbps.

2.2.3 Status LED

The status LED will display to the operator whether the node has been able to connect to the network.

Requirement: The status LED must be clearly visible from 3 meters away with a drive current of 10mA.

2.2.4 Connect button

The single button on each node will allow a user to connect to the network and provide limited interaction with its setup.

Requirement 1: The connect button must be easily-pressible.
Requirement 2: Must not have accidental mechanical failures when dropped.

2.3 WiFi Module

Data from the control module is sent via UART to be accessed on a WiFi network. A WiFi SoC (System-on-a-Chip) operates off SPI flash program memory and uses an antenna for both receiving and transmitting.

2.3.1 Antenna

A 2.4GHz PCB trace antenna will be optimized to allow for maximum throughput and a maximum range. We will aim for 10Mbps access at 800ft. This is within the capabilities of the WiFi IC and is dependant on the match and design of the antenna.

Requirement 1: The antenna must be matched at 50 +/- 20% between 2402-2484MHz.
Requirement 2: It must provide >-75dBm access at 800ft open-field with +19.5dBm input power.
Requirement 3: Antenna must be omnidirectional to within ~6dB.

2.3.2 WiFi IC

We have chosen our WiFi IC, the ESP8266, with cost in mind. This chip includes a 32-bit microcontroller and WiFi transceiver. This was chosen since it costs 5-10 times less than competitors, but it sacrifices some performance and is a bottleneck in our design. It operates at 160MHz (overclock) and has a data input communication with the PIC32 microcontroller via UART.

Requirement 1: The WiFi IC must be able to communicate over IEEE 802.11b/g/n at >100kbps with a 50 nominal RF connection.
Requirement 2: It must be able to communicate over both SPI and UART.

2.3.3 Flash

The flash IC holds the program memory for the WiFi IC. It must operate at 80MHz for the WiFi microcontroller to operate at full speed. Although we do not know our current program size for this microcontroller, we will prototype a size of 1MB and downsize (for cost savings) if possible.

Requirement: The program memory flash must have >=1MB of storage, and operate reliably at 80MHz.

2.4 Server

The server design will consist of a Raspberry Pi, a cellular receiver, a WiFi dongle, and an external hard drive. We will not consider it in the scope of this class, though it is integral for our project to connect to the greater internet.

2.5 Risk Analysis

The WiFi antenna is a significant risk to the successful completion of this project. The PCB trace antenna's ability to receive and transmit signals within the 2.4GHz 802.11b/g/n band is key for a useful network. It must be able to communicate within a useful range of several hundred feet in all orientations and directions (relatively omnidirectional and unpolarized). We will need to design the PCB trace antenna for a good match to the WiFi IC while maintaining an omnidirectional beam pattern with gain high enough to communicate with other nodes hundreds of feet away. These requirements are difficult to meet because they rely largely on antenna trace dimensions, board layout, and discrete high-frequency design.

Antennas can be "impedance-matched" via a network of inductors and capacitors, minimizing losses. If the antenna is not well-matched, excess power will become noise in the system and will decrease the range and potential throughput. We require that the impedance be as close to 50Ω as possible, which transfers the maximum amount of power between the WiFi IC and the antenna for both reception and transmission. The impedance can be modified by changing inductors and capacitors in the antenna's matching network, which we will experiment with to achieve optimal values. We can also adjust the frequency response of the antenna by modifying the copper that makes up the antenna.

The directivity of the antenna is a function of many different variables, including the PCB and type of antenna. We will choose an omnidirectional antenna topology and design our PCB as to minimally interfere. If the antenna is highly directive (with most of the sensitivity in one direction, and poor performance everywhere else), we can modify the antenna trace with copper tape or a knife.

3 Safety and Ethics

There are several potential safety hazards with our project. Lithium-ion batteries can explode if overcharged or brought to extreme temperatures [10]. A li-ion cell can experience thermal runaway, where a positive feedback loop between cell temperature and discharge rate can lead to battery failure and potential explosion. To close this feedback loop, we will closely monitor cell temperature with a thermistor and isolate the battery from both the charging circuitry and the node hardware if it reaches a temperature of above 45C or below 0C. Additionally, over-charging the battery can lead to a breakdown of the cathode, a highly exothermic process. Before attaching a battery, we will thoroughly test all of our charging circuitry to ensure that the battery will not be charged over 4.21v under any circumstance.

As an outdoor electrical device, moisture could cause damage to the nodes leading to short-circuits. The case will need to adhere to strict IP67 guidelines, which keeps the internals dry in up to 1m of water.

We are responsible for the information that is sent through our technology. This spread of valuable knowledge is an implementation of the IEEE Code of Ethics, #5: “To improve the understanding of technology; its appropriate application, and potential consequences” [11]. We hope to bring education and communication to the most remote corners of the world.

Unfortunately, risks surrounding the spread of information include piracy and mental health. Every day, people pirate music, movies, and even books via the conventional internet - and there is no reason to believe that our network will be any different. We are not explicitly giving out the tools to commit piracy or copyright infringement of any kind, but in a decentralized network it is impossible to track with any degree of certainty what information is shared. This would go against #7 and #9 of the IEEE Code of Ethics - the people committing piracy are not properly crediting the work of others, and they could be injuring the copyright holders by sharing content without paying for it [11]. We do not currently have a solution to this - we do not believe it would be the right course of action to limit the utility of our network simply because we anticipate a small subset of our users engaging in piracy.

On the internet, where a certain degree of anonymity is assured, there are fewer barriers to behaviors like cyberbullying. This type of harassment will adversely affect the mental health of those on the receiving end. It is entirely possible that the network will be used to discriminate by race, gender, or sexual orientation, violating #8 of the IEEE Code of Ethics, “to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression” [11]. We plan to introduce the ability for node owners to “ban” certain devices from services hosted on their node. The “banned” user would have no knowledge of this action; their packets would simply not return a response as the node hosting the service would throw them away instead of processing them. We believe this is the best course of action - any harassment can be stopped by an automated system, and the harasser(s) will never know that their messages aren’t being delivered.

Our mitigation techniques align with the IEEE Code of Ethics, #1: “To accept responsibility...” [11]. There are many risks that present themselves as a consequence to access and free communication, but we believe that the advantages of open resources far outweigh the potential negative effects.

References

[1] Google Public Data Explorer, ‘World Development Indicators’, 2014. [Online]. Available: http://www.google.com/publicdata/explore?ds=d5bncppjof8f9_#!ctype=l&strail=false&bcs=d&nselm=h&met_y=it_net_bbnd_p2&scale_y=lin&ind_y=false&rdim=region&idim=region:SSF&ifdim=region&hl=en_US&dl=en_US&ind=false. [Accessed: 28- Feb- 2016].

[2] Ericsson, ‘Sub-Saharan Africa - Ericsson Mobility Report Appendix’, 2014. [Online]. Available: http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf. [Accessed: 28-Feb-2016].

[3] OpenSignal, ‘The State of LTE February 2014’, 2014. [Online]. Available: http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf. [Accessed: 28-Feb- 2016].

[4] Pew Research Center, ‘Broadband Technology Fact Sheet’, 2014. [Online]. Available: http://www.pewinternet.org/fact-sheets/broadband-technology-fact-sheet/. [Accessed: 28-Feb-2016].

[5] F. Brown, ‘Percentage of global population living in cities, by continent’, *The Guardian*, 2009. [Online]. Available: http://www.theguardian.com/news/datablog/2009/aug/18/percentage-population-living-cities. [Accessed: 28-Feb-2016].

[6] PewGlobal.org, 'Communications Technology in Emerging and Developing Nations', 2015. [Online]. Available: http://www.pewglobal.org/2015/03/19/1-communications-technology-in-emerging-and-developing-nations/. [Accessed: 02- Oct- 2015].

[7] Internet.org, ‘Our Approach’, 2016. [Online] Available: https://info.internet.org/en/approach/. [Accessed: 24-Dec-2016]

[8] Renewable Energy World, ‘Solar-powered Internet Connectivity in Lascahobas, Haiti’, 2012. [Online]. Available: http://www.renewableenergyworld.com/ugc/articles/2012/01/solarpowered-internet-connectivity-in-lascahobas-haiti.html. [Accessed: 24-Dec-2016]

[9] IFAD,’Rural Poverty in Nepal’, 2011. [Online]. Available: http://www.ruralpovertyportal.org/country/home/tags/nepal. [Accessed: 28-Feb-2016].

[10] D. Doughty and E. P. Roth, "A General Discussion of Li Ion Battery Safety," The Electrochemical Society Interface, Summer 2012.

[11] Ieee.org, "IEEE IEEE Code of Ethics", 2016. [Online]. Available: http://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 29- Feb- 2016].