Sandia National Laboratories Clinic Team

Matt Strum
(Zach Smart, Jake Scheid, Jacob Fawson, and Ali Aldarwish)

Advisor – Behrouz Farhang

Final Project Proposal – May 4, 2011

Contents

Functional Description 2
Design Overview 2
Responsibilities 3
Design Details 3
Antenna 3
Sensors 3
Digital Signal Processing 3
User Interface 4
Server 4
Client 4
Interface Specifications 4
Risks 5
Schedule 5
Tasking 6
Billing of Materials 7
Contacts 7
References 7

Functional Description

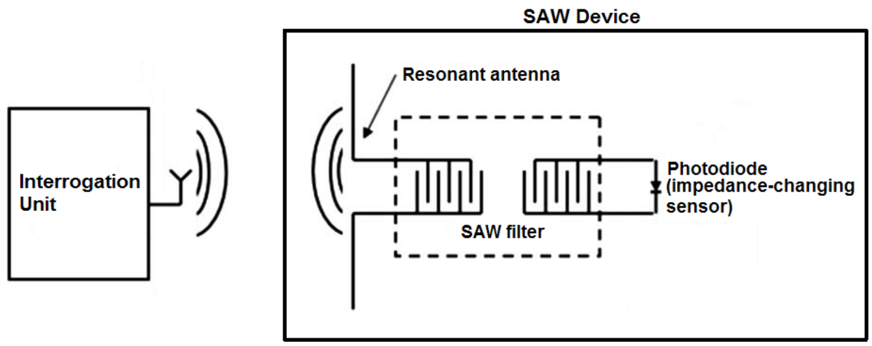
Distributed Wireless Sensor Networks

We will incorporate passive sensor tags into a functional distributed network. This will be accomplished by creating at least three different types of cheap, small, passively-powered sensors along with a transmitter/receiver (interrogator) which is able to both provide power wirelessly to the sensors and read and process the output.

Our usage scenario is preventing assets within a closed facility from being removed. We want to be able to put our sensors on an asset, like a USB drive, without any need to worry about a power source or battery life. The interrogator(s) would then most likely be located near any exit. Once powered on, the interrogator unit would constantly send and receive wireless signals to any asset within the transmitting range. That data would then be processed and transmitted wirelessly so that a security task force could monitor and act on the data.

Design Overview

Here is a diagram showing the general architecture [1]:



The interrogator will transmit a sweeping signal within a predefined frequency range. That signal will be received by sensor devices with antennas designed for specific frequency ranges. The signal passes through a Surface Acoustic Wave (SAW) filter which produces a surface wave. That surface wave passes through a sensor, like a photodiode, which alters the wave by acting like a load. After passing through the sensor the surface wave is transformed back into a signal by exiting through the SAW filter and being sent back to the interrogator unit.

The interrogator unit will perform some simple Digital Signal Processing (DSP) by analyzing the received signals, separating the separate sensors, and evaluating the values. If anything of interest is detected, like a new sensor being found in range or a change in value, the interrogator unit will transmit a packet of data across the local wireless network so that any listening clients, like a security guard using a tablet computer, on the network can receive the new data.

Responsibilities

Zach Smart, Jake Scheid, Ali aldarwish, and Jacob Fawson are responsible for everything from transmitting the signal to the sensors to receiving the signal back after it has passed through any sensor within range. The bulk of the work will be antenna design.

I will be responsible for processing the signal and getting it to a user. The rest of the team will assist me specifically with interfacing between the DSP logic and the interrogator.

Design Details

Antenna

Because we need our sensors to be passive, our choice of antenna is extremely important. We have ordered SAW (Surface Acoustic Wave) tags and will soon start working with them. For initial tests we will simply hook up the sensor tags to a network analyzer. Appropriate antennas will also need be designed for the interrogator, which transmits a wave which powers the sensors and receives signals back. The antennas will be designed to work in the VHF and/or UHF ranges. We have ordered sensor tags in various frequency ranges. We will select three frequencies which will be used and create antennas for them.

Another variable factor is that our antenna can be rigid or flexible since it's passive. We have initially decided to go with a rigid design which should simplify the antenna design. Flexible designs are much harder to create so we will just plan for a rigid design and leave any possibility for a flexible design to if we have time to do it.

Sensors

The sensors will connect between the receive and transmit antennas located on the substrate. As the sensor values change, so will the resistance. We are going to test out some different sensors to see which would be advantageous to use. Types which are currently in consideration are: temperature, pressure, sound, and light. We are hoping that if we create a baseline for the sensors that we will be able to have sufficient resolution. In order to get the strongest signal differences we will need to make sure that the antennas work where there is minimal interference.

Initial testing will be done using a potentiometer connected to the sensor tags we have ordered.

Digital Signal Processing

The first major component of the computing end of our project is the DSP. The interrogator unit, along with the already mentioned antennas, will also be accompanied by a small-form factor computer. For the DSP we will need to differentiate and characterize the signals from the three different types of sensor tags and create a baseline to compare against and implement. The differentiating of the signals will just be dealing with sensors which operate at different frequencies. Matlab which will be running on the computer will be in charge of doing the DSP work.

Depending on how strong or weak the signal is we will need to add some amplification and filtering to the signals received from the sensors.

The initial work will involve investigating the sensor signal data which has been collected by Sandia Laboratories. The head engineer who has completed a test run using a SAW sensor he assembled provided us with raw data which we should be able to use to start working on the DSP. I will need to contact the Sandia engineer and confirm how I will be able to read and process the data.

Once we have established how a signal will look and are able to differentiate different signal levels then we should be able to adapt our model fairly easily for any changes to the sensor loads, frequencies, etc. Although we will need to edit our model to work in the real world instead of a simulation we will keep our simulated model working so that it can be used in a demo by the end of Fall semester.

User Interface

The small form factor computer which does the DSP processing will not have any user interface associated with it. A user will be able to connect video and input to it to install or configure software as needed, but when being used in the field there will be no user interactions with the interrogator. Data will be broadcasted from the interrogator over an 802.11 wireless connection to any client on the network. Due to this architecture, there will be two portions to work on: the server running at the interrogator and the client running on a mobile device. This is the aspect of the project I am personally interested in.

Server

The PC will decide when to send data to the client, perhaps a combination of interval and important updates. The initial design is to simply broadcast to a custom port on the local network so that any local device will be able to get updates. Possible features could include some sort of authentication so that only authenticated devices could receive updates. Because our scenario is using interrogators within an environment which probably already uses an encrypted network, building in authentication won’t be part of the official goals. If time permits, I will add a public/private key encryption scheme where the private key is distributed only to devices which should be able to read the updates from the server.

Client

A client which will receive the status updates over 802.11 will also be developed. This will involve creating an Android program to receive and present the data to a user in a meaningful way. Like it was mentioned in the server section, the default implementation will simply listen for broadcast packets of data on the network using the custom port and if time permits a public/private key encryption system will be added.

Interface Specifications

The interrogator will have an input coming from wherever the signal is being received, either a network analyzer or elsewhere. The connection will most likely be RS-232 or USB. The group is going to investigate the sensor tags over the summer and determine what will be best.

Packets of data will be sent over 802.11 and will contain simple datagrams.

Risks

Our main risks which I can think of are:

- Antennas
  - Signal strengths
  - Interference
- DSP
  - Learning curve
- Server/Client
  - Android programming

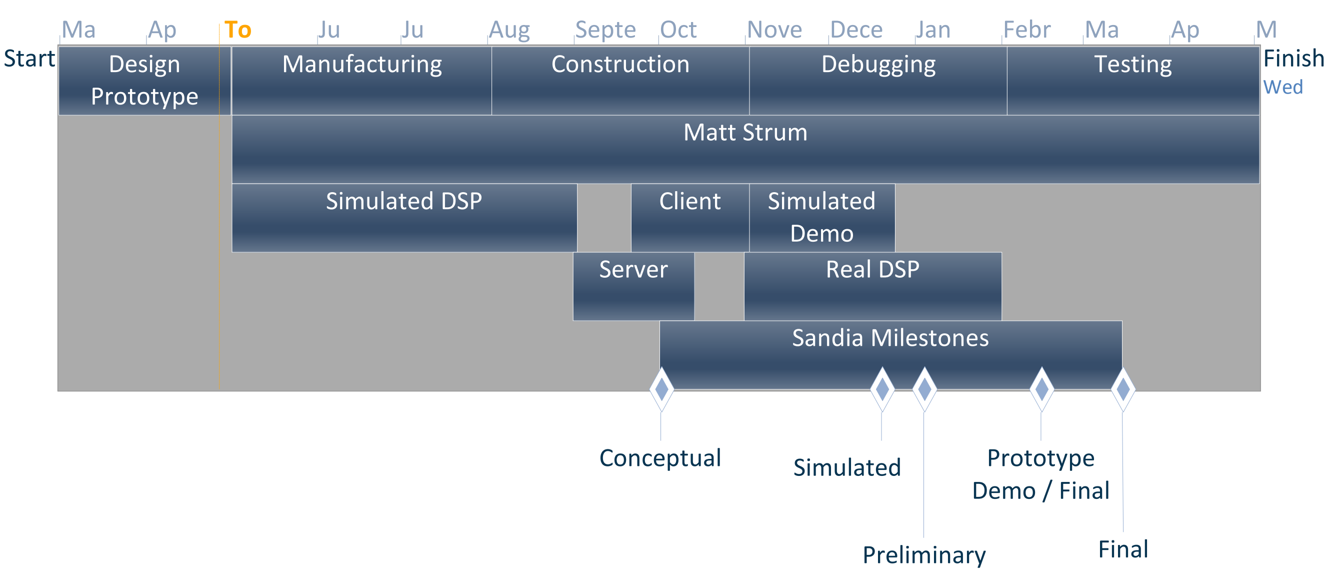
I don't see too much risk once we can actually figure out how to characterize and process the signals, but that is going to be a huge task. The server/client model shouldn't have any problems and I don't perceive any large risks.

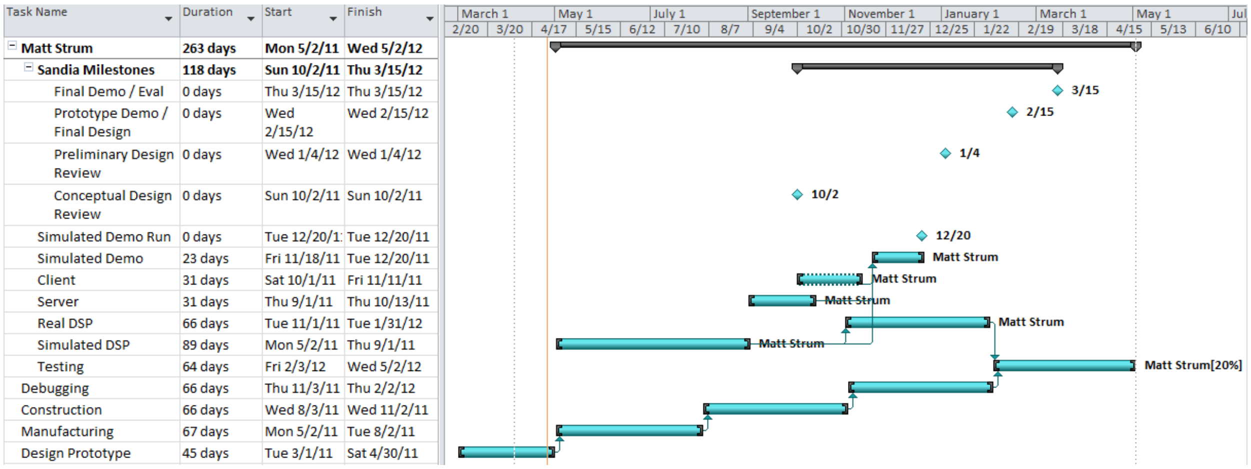
Schedule

Here are some key dates suggested by Sandia Laboratories:

Key Dates	Event
February 8, 2011	Kick-off meeting
March 31, 2011	Follow-up meeting
September, 2011	Meeting
October 4, 2011	Conceptual design review
December/January, 2012	Preliminary design review
February, 2012	Prototype demonstration and final design review
March, 2012	Final demonstration and evaluation

I have taken the group's Gantt chart and augmented it with my own personal tasks:





Task Name	Duration	Start	Finish
Matt Strum	**263 days**	**Mon 5/2/11**	**Wed 5/2/12**
Sandia Milestones	**118 days**	**Sun 10/2/11**	**Thu 3/15/12**
Final Demo / Eval	0 days	Thu 3/15/12	Thu 3/15/12
Prototype Demo / Final Design	0 days	Wed 2/15/12	Wed 2/15/12
Preliminary Design Review	0 days	Wed 1/4/12	Wed 1/4/12
Conceptual Design Review	0 days	Sun 10/2/11	Sun 10/2/11
Simulated Demo Run	0 days	Tue 12/20/1	Tue 12/20/11
Simulated Demo	23 days	Fri 11/18/11	Tue 12/20/11
Client	31 days	Sat 10/1/11	Fri 11/11/11
Server	31 days	Thu 9/1/11	Thu 10/13/11
Real DSP	66 days	Tue 11/1/11	Tue 1/31/12
Simulated DSP	89 days	Mon 5/2/11	Thu 9/1/11
Testing	64 days	Fri 2/3/12	Wed 5/2/12
Debugging	66 days	Thu 11/3/11	Thu 2/2/12
Construction	66 days	Wed 8/3/11	Wed 11/2/11
Manufacturing	67 days	Mon 5/2/11	Tue 8/2/11
Design Prototype	45 days	Tue 3/1/11	Sat 4/30/11

Tasking

1) Antenna – Zach Smart, Jake Scheid

Each of the sensor tags is calibrated for a different frequency, so they will need to create antennas for the sensor tags we'll be using.

2) Sensors – Jacob Fawson, Jake Scheid

We have received a couple of SAW sensor tags from DigiKey and are ready to start testing them. They will be testing out hooking various sensors to the tags to see how everything works.

3) Matt Strum, Ali Aldarwish

First off, we will need to get experimental data and figure out the best way to process it. Sandia Labs has experimental data which we can use which mimics what we would get back from these wireless sensor tags. Once we're able to characterize the signals we should have a better idea of what do to for the DSP and PC portions of the interrogator. We will most likely use LabView or Matlab to process the data to try and get useable output. We should also be able to tailor our algorithms once we are able to characterize some sensors. This is what I will be doing in the summer as noted on the schedule above. Since I have an internship I won't have as much time to dedicate to the project for a while.

The other portions of the project include creating the server and client model for transmitting and receiving updates. This should just involve standardizing how to put the data into the IP packets, transmit it from the computer, and monitor for packets on either an Android device or simply another PC.

The timeline and milestones for my particular tasks are included in the above chart along with the group's initial schedule.

Billing of Materials

Item	Quantity	Description	Price	Total
1	1	Network Analyzer - U of U Microwave lab	$0.00	$0.00
2	20	Sensor tags in the VHF and UHF frequency	$10	$200
3	1	Mat lab - U of U Microwave lab	$0.00	$0.00
4	7	SAW Antennas	$15	$135
5	2	Proto-board	$50	$100
6	1	VIA ARTiGO A1100 PC + HD/Memory	$500	$500
7	1	Substrate for System Mount	$20	$20

The sensor tags will be bought from DigiKey Corp by the team members who are working on that part of the project.

The VIA ARTiGO A1100 PC is available from E-ITX (510-770-9419) and will be shipped with all the hardware added to the original A1100 DIY PC which doesn't come with the memory or hard drive.

Contacts

Sandia

Steven Paradise
sparadi@sandia.gov
925-294-2755

Lisa Andersen
landers@sandia.gov
925-294-2580

Advisor

Behrouz Farhang
farhang@ece.utah.edu
(801) 587-7959
MEB 4510

References

[1] Steven Paradise, Lisa Andersen, "Distributed Wireless Sensor Networks," Power Point Presentation for Sandia National Laboratories Clinic Instruction, 2011.