Proposal: Analysis of Electromagnetic Interference on Medical Devices

John Backes and Bob Guidinger

Department of Electrical and Computer Engineering
Department of Computer Science
University of Minnesota
200 Union St. S.E., Minneapolis, MN 55455
{back0145, guidi002}@umn.edu

I. Motivation

More and more patients are relying on implantable medical devices for treatment. According to the American Heart Association, pacemakers are currently implanted in at least 3 million people, and 6 hundred thousand more are implanted every year [8]. Previous work has shown the lack of security in the communication protocols used by medical devices [5], [2], [4], [6]. However, these types of security flaws are generally specific to a particular device.

The Food and Drug Administration has warned against the possible negative effects of Electromagnetic Interference (EMI) on medical devices [9]. Although these reports show that there have been few cases where EMI generated from commercial devices has caused harm to a patient, the study doesn't discuss the ability of a malicious adversary from disturbing medical devices with EMI. Other studies have focused on the effects of EMI given off by cell phones on pacemakers [1], [3].

In this work, we will explore the effects of EMI on a device with sensors similar to some implantable devices. The goal of this project is to see if we can use commercially available tools to generate a significant enough amount of of EMI to disrupt the analog sensors on a device.

II. Scope

A. What is in the scope of this project?

In this project we will attempt to quantify the amount of EMI (in power and frequency) that is needed to "disturb" the analog sensors on a wireless mote. We will consider a sensor to be "disturbed" if its recorded measurement is *significantly* different from the actual correct values. For example, if we are able to make the temperature sensor have a reading that differs by at least 15% from the correct value, we would consider it to be disturbed. However, if the measured value only differs by less than 15%, we would not consider the device to be disturbed. The following sensors that we will attempt to disrupt are:

1) Temperature Sensor
2) Acoustic Sensor
3) Battery Level Sensor
4) Light Sensor
5) Any Unused ADC inputs

If possible, we may also see if we are able to disrupt any of the digital circuitry on the device. This will be much more challenging because the voltage levels that need to be generated to disturb the digital circuitry will be much greater than the analog circuitry.

B. What is **not** in the scope of this project?

In this project we will not try to reverse engineer or disturb any of the wireless communication protocols used by the motes.

III. Experiment

In the first experiment, we will attempt to affect the readings on the microphone on the MTS300CB Sensor Board. This device will likely be easier to affect because unlike the other devices, this sensor samples an AC signal.

A. Setup

Our experimental setup is shown in Figure 1. We will use a waveform generator to send a modulated RF signal towards the microphone on the device. We will then attach an oscilliscope with a spectrum analyzer to the output of the amplifier attached to the microphone on the PCB.

B. Steps

The following steps outline our process given the experimental setup shown in Figure 1.

1) Attach longer leads to the microphone (perhaps 4cm and 8cm). The longer the leads, the more EMI the microphone will pickup. Antennas tend to pick up signals that have a wavelength that is an even factor of the antenna length (e.g., half the wavelength or a quarter of the wavelength). To give some perspective, a 500 MHz signal has a quarter wave length of 15cm.
2) Program the mote to record audio signals within the 20Hz-20kHz range. The program can either send the data directly to the computer or can keep a log of the data in flash memory.
3) Create a baseline recording for the microphone without any interference.
4) Move the signal generator's antenna very close to the device.
5) Use the waveform generator to send an RF signal with a frequency that has a quarter wavelength equal to the length of the microphone leads. This signal will be modulated with a lower frequency signal in the 20Hz-20kHz range. Both the carrier signal and the modulated signal can be adjusted to discover the most effective way to generate a signal that appears at the output of the microphones amplifier.

IV. Procedure

Here we outline a rough sketch of the procedure and work distribution for completing the project. Many of the tasks between Bob and John can be done in parallel.

A. John

1) Study RF concepts and write proposal (1 week)
2) Perform generic EMI tests with equipment (1 week)
3) Perform EMI test on different traces on the PCB (1 week)
4) Develop programs for reading sensors (1 week)
5) Write interim report (1 week)
6) Test shielding strategies (2 weeks)
7) Run EMI tests with new strategies (1 week)
8) Write final report (1 week)

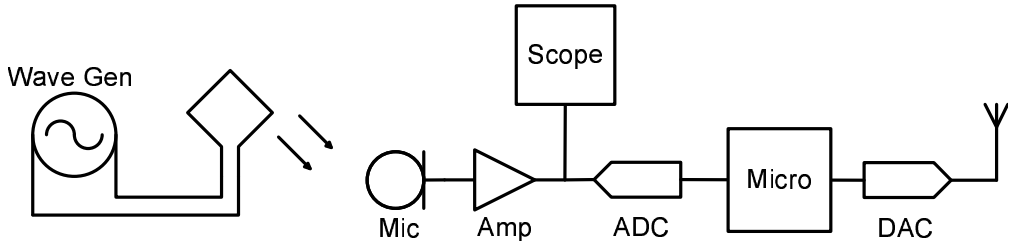

Fig. 1. The experimental setup

B. Bob

1) Read TinyOS/Mote documentation and write proposal (1 week)
2) Develop programs for reading sensors (2 weeks)
3) Test measurements under EMI (1 week)
4) Write interim report (1 week)
5) Develop software strategies to mitigate/test for EMI (2 weeks)
6) Run EMI tests with new strategies (1 week)
7) Write final report (1 week)

V. Resources

A. Reading Materials

1) *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses* [5]
   This paper talks about some of the challenges with securing a medical device. However, most of the "meat" of this paper deals with hacking the communication protocol and wont be directly relevant for the type of attack that we would be implementing in this project
2) *The ARRL Handbook* [7]
   A reference guide for generating radio signals and constructing antennas. This will be useful for figuring out how the power/frequency ranges that will be necessary to cause a meaningful disruption in the device.
3) *http://www.tinyos.net/*
   This website contains guides for programing the motes
4) *MPR-MIB Users Manual*
   Contains electrical specifications and formulas for reading sensor values from the motes

B. Equipment

1) *Oscilloscope*
   A scope will be used to view the signals induced by EMI on the PCB for the mote. We already have access to some scopes.
2) *Function Generator*
   A function generator will be used to generate the EMI. This is the most crucial and likely hard to obtain piece of equipment we will need for this project. We currently have access to some older devices that may or may not be adequate for generating the frequencies and power levels that we will need to create significant interference. I believe the communications labs on the third floor have function generators with the specifications that will suite our needs.
3) *Antenna*
   The antenna will be attached to the function generator to transmit the signals at the mote. There is a lot of rich theory related to how shaping the antenna can increase the broadcast range and strength of a signal. However, optimizing the antenna will likely be beyond the scope of this project. The communications lab will likely have antennas that are suitable for this project. We can also experiment with some ideas presented in the ARRL Handbook [7] (available for free at the library); we could probably get some cheap materials for this at Axe Man.
4) *Two Mote's, a Sensor Board, and a Programmer*
   These have already been provided for us. We will write a program on the mote to transmit readings from its analog sensors to a computer.
5) *Computer*
   A computer will be used to program the mote and also to read the data from the analog sensors on the mote. To keep the environment consistent in case we need to use multiple computers, we will be using a virtual machine with the TinyOS distribution installed. We have already set up this environment and used it to successfully program a simple "Hello World" type program on the mote as a proof of concept.

C. Personnel

During this project we will be actively working with Denis Kune. We will have weekly meetings with him to discuss the progress of the project, and we will use his expertise to help solve some of our problems.

References

[1] V Barbaro, P Bartolini, G Calcagnini, F Censi, B Beard, P Ruggera, and D Witters. On the mechanisms of interference between mobile phones and pacemakers: parasitic demodulation of gsm signal by the sensing amplifier. *Physics in Medicine and Biology*, 48(11):1661, 2003.

[2] Anthony Bellissimo, John Burgess, and Kevin Fu. Secure software updates: disappointments and new challenges. In *In USENIX Workshop on Hot Topics in Security (HotSec*, 2006.

[3] Federica Censi, Giovanni Calcagnini, Michele Triventi, Eugenio Mattei, and Pietro Bartolini. Interference between mobile phones and pacemakers: a look inside. *Ann Ist Super Sanita*, 43(3):254–259, 2007.

[4] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 conference on SIGCOMM*, SIGCOMM '11, pages 2–13, 2011.

[5] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy'*, pages 129–142, 2008.

[6] Daniel Halperin, Thomas S. Heydt-benjamin, Kevin Fu, Tadayoshi Kohno, William H, Daniel Halperin, Tadayoshi Kohno, Thomas S. Heydt-benjamin, Kevin Fu, William H. Maisel, and Beth Israel Deaconess. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, 7(1):3039, Jan.Mar*, pages 10–1109, 2008.

[7] American Radio Relay League. *The ARRL Handbook*. The American Radio Relay League, Inc, 2010.

[8] MD Mark A. Wood and MD Kenneth A. Ellenbogen. Cardiac pacemakers from the patient's perspective. *Circulation*, 105:2136–2138, 2002.

[9] J. Tikkanen. Wireless electromagneticinterference (emi) in healthcare facilities. *Blackberry White Paper*.