

Project Proposal

Simple RFID Spoofer

3/1/2011

Dave Marchevsky

Project Abstract

I will implement a RFID spoofer system using the ZNEO development kit, an RFID reader, and a 125khz antenna. The system will read the data and unique identifier from a RFID card, decode and store this data in memory, and allow the user to spoof the card by transmitting an equivalent signal (with the card's unique hardware ID) using the antenna. The antenna transmission part of the project will be similar to <http://www.instructables.com/id/Stupid-Simple-Arduino-LF-RFID-Tag-Spoofier/>, which is a RFID spoofer without a reader component. I will purchase an antenna online (as they are quite cheap) instead of building one from scratch, however. I will also investigate spoofing HID proximity cards, which operate on a different frequency and with slightly different parameters. Reading and spoofing these cards will likely require a different reader and antenna setup, as well as different encoding, decoding, and transmission functions, but the concept would be identical.

Strategy

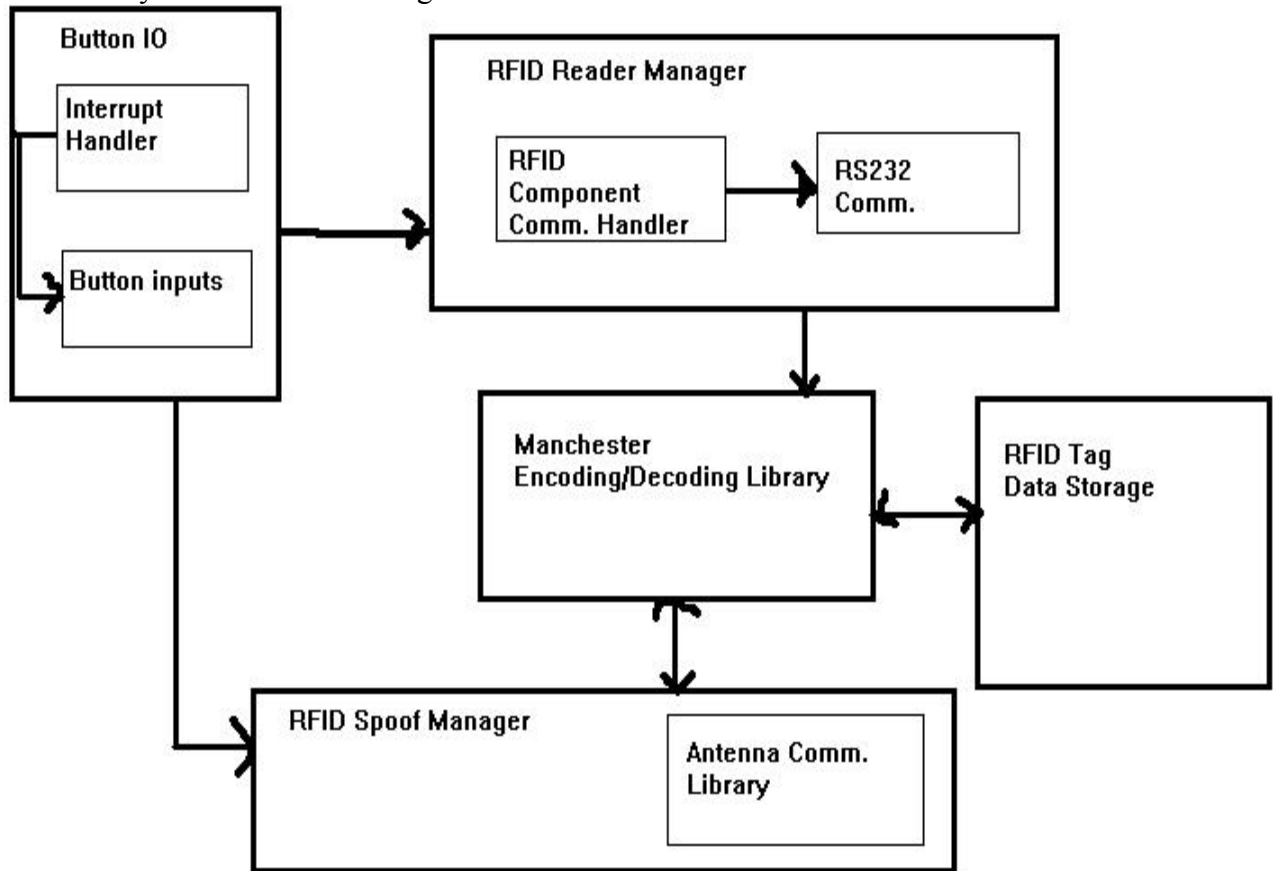
I will be using the ZNEO Contest Kit Development Board as the microcontroller for this project. The system will take input from an RFID reader component with internal antenna, which will pass information to the system via a RS232 signal. The system will decode the Manchester-encoded data provided by the reader and store this information in memory. It is not strictly necessary to decode the provided information since the basic system will just be transmitting the encoded data again, but if I have time I will implement a computer interface to the system that will allow storage of the data on a computer, as well as downloading data to the reader.

I will be using interrupts to clock the antenna frequency properly, to clock the reader component, to display text information using the LEDs, to debounce the buttons for the user interface, and surely many other things.

Reviews of the reader component on Sparkfun are very positive so I am sure it will work. Also a similar system has been implemented on Arduino using the reader component, so I know it will work properly. The antenna is simply a coiled copper wire, so I just need to send the right signal over it at the right rate and it should transmit properly. If there is a problem with the antenna I can simply build my own.

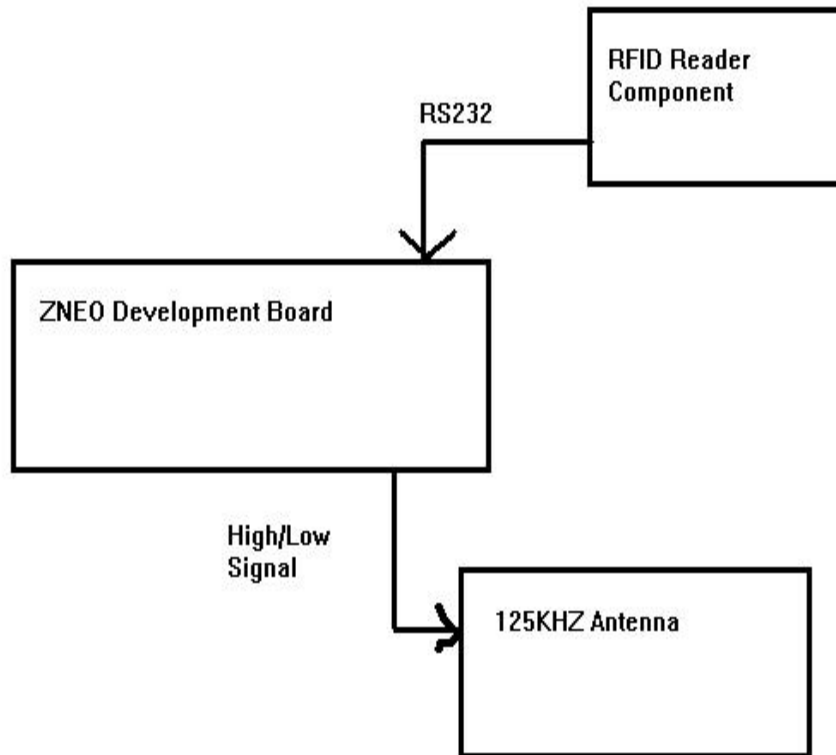
I will need to write a text display module (will adapt the hello world lab) to display info about the state of the system, a button control module to allow switching between read and write modes, an encoder/decoder module to deal with Manchester encoded data read in and to be transmitted using the antenna, a RFID reader module to communicate with the reader component, and an antenna transmission library to abstract away antenna hardware details.

Preliminary Software Block Diagram:



Preliminary Hardware Block Diagram:

Preliminary Hardware Block Diagram



Unknowns

I anticipate that reading the RFID information will not be very challenging, as I'm going to buy a pre-built component that will do this for me. I will, however, need to ensure that I read the RFID tag information properly and deal with the Manchester encoding.

The hardest part of the project will no doubt be the antenna testing and signal transmission. The instructables link in the abstract describes a rough implementation strategy for the antenna and has links to further information, but I would like to purchase an antenna and focus on maximizing the transmission strength and quality. I will probably be spending some quality time with the oscilloscope testing out my antenna current.

I initially planned on building my own antenna like the instructables link described, but I discovered that a pre-built antenna is available online for less than 5 dollars. Although constructing such an antenna is fairly simple compared to more involved antennas, I have no experience at all in this field and would rather not have this impede my progress. I will still probably attempt to tweak the pre-built one to increase transmission range.

Implementation Plan

I plan to complete my project in the following order: I will first create a working

Project Proposal
David Marchevsky
Embedded Systems Spring 2011

RFID reader using the ZNEO and the reader component that I will purchase online. The RFID reader will read and store the RFID card's information and unique ID. This will require an understanding of the RFID transfer protocol and a function to decode the Manchester-encoded data.

After I have this working I will hook up the antenna to the ZNEO and attempt some simple transmissions. As the antenna is the most likely source of error in my system, I will test it extensively to ensure that it transmits properly over a reasonable range.

Finally, I will hook up the antenna to the ZNEO via the breadboard and complete the system's transmission functions. I will either purchase a second RFID reader component that I will hook up to a PC to read the spoofed signal, or read the spoofed signal with the system's built-in reader to test my system. Tweaking the timing of the signal and the frequency and construction of the antenna will be critical to producing a good transmission. The milestone chart is as follows:

Task	Time estimate
Build ZNEO RFID reader system	2 weeks
Connect antenna/do simple tests	1 week
Test basic antenna transmission	1 week
Integrate antenna into RFID reader	1 week
Tweak and test the completed system	2 weeks
TOTAL:	7 weeks

Resources

For my project I will need: the ZNEO contest kit (development board and breadboard), RFID reader component (possibly two, one for PC), RFID test cards (must be compatible with reader), wire antenna, the ZNEO SDK and C compiler, and some wire to hook up the reader module to the ZNEO input via the breadboard.

I already have the contest kit, wires to hook up to ZNEO input, the SDK and the C compiler. I will need to purchase the reader and sample cards as well as the antenna wire. The RFID reader and cards are available at sparkfun, and the antenna is available here: <http://store.qkits.com/moreinfo.cfm/AN0201>. All the components that I need to purchase should have a total cost of less than 40 dollars, shipped, so they will not be hard to obtain.