RFID Tunnel

6.101 Project Proposal
Spring 2014

Vineel Adusumilli
Austin Duffield
Brandon Vasquez

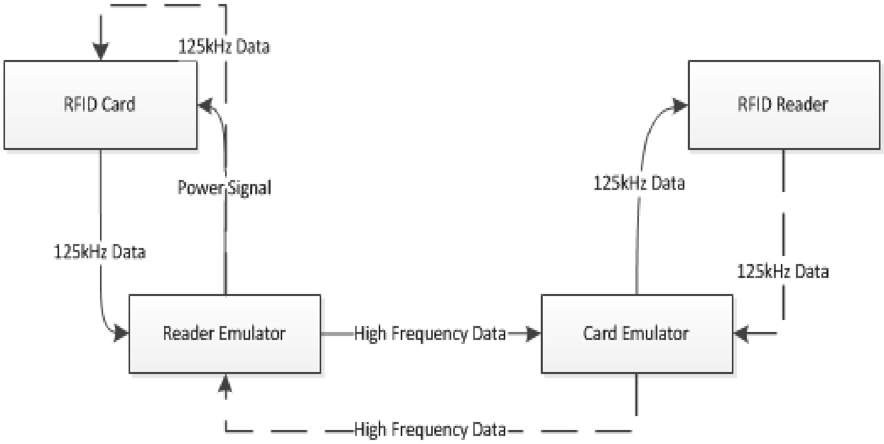
Overview

Our project is meant to demonstrate a fundamental security flaw in RFID: readers have no way of verifying that the card is physically present. We plan to demonstrate this by using our system with MIT ID cards to open doors from a distance.

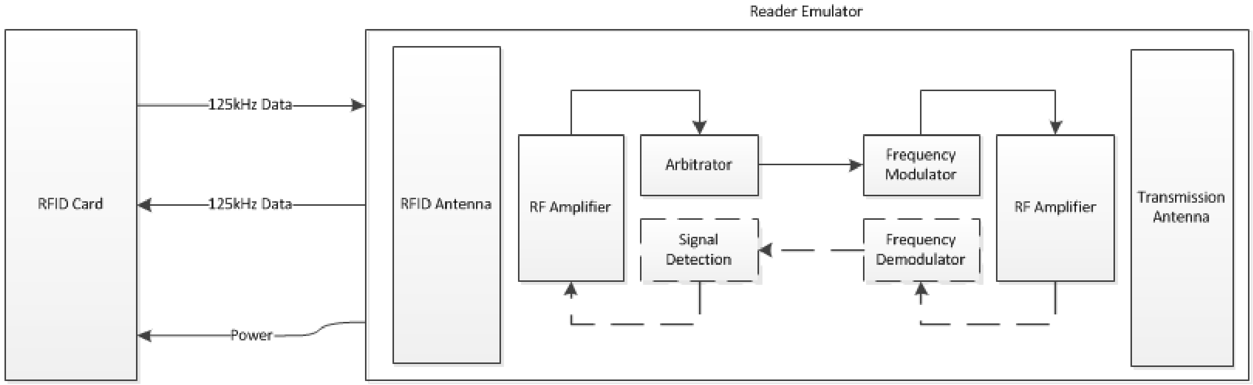
The RFID Tunnel will relay an RFID signal over a considerable distance by acting as a bridge between an RFID card and an RFID reader, specifically using 125KHz MIT ID cards and readers. There will be two distinct physical devices: a reader emulator and a card emulator. The reader emulator will be placed near a card, exciting it and sending any output data over an RF link to the card emulator, which will be placed near a reader. The card emulator will then convey the received information to the actual reader. Both the reader emulator and card emulator will be designed to be low power and portable, yet still able to transmit a signal over a reasonable distance.

System Block Diagram

The main goal of this project is to implement one way communication between an RFID card and a base station. The critical path is the solid lines. An extension to this project, time permitting, would be to implement two way communication, the dotted lines, which would bring on new challenges like using two different transmission frequencies and detecting when to receive and transmit data for RFID systems that use a handshake.

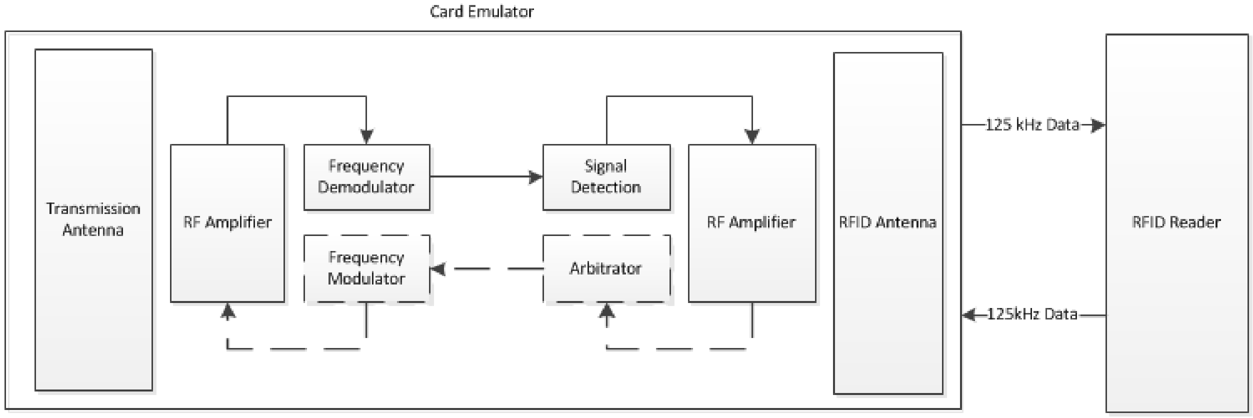


Reader Emulator



The Reader Emulator is tasked with exciting the RFID card and pretending to be the RFID reader. It will have a RF power amplifier connected to the RFID antenna which will provide power wirelessly to the RFID card. The 125KHz sine wave output by the reader emulator will be attenuated by the card, generating a data signal. This signal will then be modulated into a higher transmission frequency, which will then in turn be amplified and transmitted over an RF antenna to the Card Emulator.

Card Emulator



RFID readers excite cards by broadcasting a sine wave of their resonant frequency (125 KHz in our case). They then "read" the card by monitoring current draw, as the card will short itself in order to convey information, causing it to draw more current from the reader.

Our card emulator will start by taking an RF signal output by the reader emulator. It will then demodulate the RF signal to recover the original RFID signal. The original RFID signal will then itself be demodulated and fed to the input of a triac or similar component which could short the AC transmission from the actual reader.

Transmission

Directional antennas are used to maximize the efficiency of the transmission and require as little power as possible for a long distance transmission. One design goal is for the reader emulator to be small and easily disguised, so that reading an ID can be discrete. This goal will inform the antenna design, but we generally find that cumbersome antennas are less of a challenge than large power consumption. As such, the transmission power is limited to 5W for a desired range of 200ft.

After receiving a 62.5khz data signal from a card, the reader-emulator must transmit this data to the card-emulator. The data transmission requires modulating the signal into the VHF band, around a 144MHz carrier, amplifying to sufficiently to travel several hundred feet, receiving the signal, and demodulating it again to get the same 62.5khz data.

The 144MHz carrier is generated by a crystal oscillator at 36MHz, which goes through two frequency doublers in order to achieve the full carrier frequency. This signal is then amplitude-modulated by the 62.5khz signal out of the card. The resulting signal is amplified in a linear manner and put on a directional 2-meter antenna. The receiver uses a similar antenna to receive the signal and a low pass filter to capture the envelope of the AM signal. The resulting signal is fed into the card emulator.

Power

Our system will be powered off of a lipo battery at 11.1V, then regulated to the voltage requirements of various parts of the circuit. The high current output from the battery is necessary for radio transmission over long distances. Rechargeability is also important as it permits the device to be reused over a long period and removes a constraint on the package - the battery doesn’t have to be removed.

Testing and Demonstration

In order to test the reader emulator, we plan to look at the input to the RF modulator using an oscilloscope to see if it matches the RFID signal that would have been read by an actual RFID reader.

In order to test the card emulator, we plan to use an Arduino to replay pre-recorded values into the card emulator. We will then read the card emulator with an actual reader and check to make sure it interprets the same values as are sent by the arduino.

In order to test the RF transmission, we plan to send and replay an audio signal.

In order to test and demonstrate our entire system, we plan to use our RFID tunnel to effectively extend the range of an Arduino-based RFID reader. The Arduino will be set up to blink an RGB LED either red, green, or blue based on which one of three cards we present to it. We will then show that the behavior remains the same when we present the cards through the RFID tunnel: the Arduino will still blink the correct color when the corresponding card is presented to the other end of the tunnel.

Breakdown of Labor

Vineel will be primarily responsible for implementing the RFID technology in the card emulator. This involves replicating the signal processing used by cards to transmit a data signal.

Brandon will be primarily responsible for implementing the RFID technology in the reader emulator. This involves designing the power amplifier and oscillator to power the RFID card, as well as signal processing for receiving the data signal.

Austin will be primarily responsible for implementing the RF transmission between the card emulator and reader emulator. This involves designing the power amplifiers and modulation for 144MHz, as well as antennas.

Conclusion

Our project will consist of two separate modules which would bridge the physical gap between an MIT RFID card and a MIT RFID reader. The card reader module will trick the base station into thinking its the physical MIT RFID card and the reader emulator will trick the MIT RFID card into thinking its the MIT reader.
This project is significantly complex and has unique risks and challenges, many of which we have not individually encountered before. One such challenge is effectively powering the RFID card wirelessly. Another is transmitting the card data over a reasonable distance between our two modules while maintaining the integrity of the data. However, our system is designed to be modular, and will be at least partially functional with just a few of the subsystems. We believe our project has great potential and look forward to the weeks ahead.

References

Josh Mandel, Austin Roach, Keith Winstein, *MIT Proximity Card Vulnerabilities* 2004:
http://web.mit.edu/keithw/Public/MIT-Card-Vulnerabilities-March31.pdf