Working with RFID Tags—
An Introduction to the proxmark3

Jonathan Westhues

user `jwesthues`, at host `cq.cx`

1 Overview

I intend this document as a brief introduction to my proxmark3 hardware. In addition to this, I will try to describe the signal processing that this device must perform. In concept this is the same correlation that any digital radio receiver performs; some details are fundamentally specific to the kinds of signals involved in an RFID system, and some are specific to my implementation.

The proxmark3 is a test instrument capable of manipulating RFID tags in a number of different ways. For example, a proxmark3 can:

> read almost any low-frequency (∼100 kHz) or high-frequency (13.56 MHz) tag, including the ISO-standard tags;
>
> emulate a low- or high-frequency tag, appearing almost indistinguishable from a real tag; or
>
> eavesdrop on the signals exchanged between another reader and tag

When the reader wants to receive a signal from the tag (whether we are reading an ID-only tag, like a prox card, or whether we are expecting some response that is a function of some message that we previously sent to a 13.56 MHz ISO-standard tag), it transmits only the unmodulated carrier that powers the tag. The tag transmits its message by alternately making the circuit across its antenna look more like an open, or more like a short (or, equivalently, by changing the resonant frequency of its antenna circuit, by disconnecting or reconnecting some inductance or capacitance to the antenna; the reader 'sees the tag more' when the tag's antenna resonates closer to the frequency of the energizing carrier).

The reader sees a lower voltage at its antenna when the tag's antenna is 'more shorted.' This means that the tag can amplitude-modulate a subcarrier onto the carrier transmitted by the reader, by varying the

It looks at the received signal on its antenna—possibly, but not necessarily, the same antenna used to transmit—and demodulates this signal

In a sense, the circuit that interprets the signal returned from the tag is a radio receiver like any other. The major peculiarity in this application is that our transmitted carrier will always bleed through, because it is so much more powerful than the information-bearing signal returned from the tag. We can consider the signal at the reader's antenna as having the form

$$v(t) = (A_c + v_s(t))(\cos \omega_c t) = A_c \cos \omega_c t + v_s(t) \cos \omega_c t = v_{tx}(t) + v_{rx}(t)$$

where A_c is the amplitude of the transmitted carrier, ω_c is the carrier frequency (125 kHz or 13.56 MHz), and $v_r(t)$ is the subcarrier amplitude-modulated onto the transmitted carrier by the tag. Only the signal $v_r(t)$ carries information; the $A_c \cos \omega_c t$ term serves only to power the tag, but it still appears at our antenna. The subcarrier frequencies used in typical RFID standards are small compared to the carrier frequency.[1] This means that the $v_s(t) \cos \omega_c t$ term is a relatively narrow bandpass signal centred at ω_c.

Unfortunately, the $A_c \cos \omega_c t$ term is much more powerful than v_{rx}. This must be so; only a fraction of the power that the reader transmits will make it to the tag, and only a fraction of the power the tag reflects back towards the reader will be receiverd by the reader's antenna. In radio terms, this means that we will always have to deal with a powerful in-band interferer. Our receiver must therefore have very high dynamic range. This is difficult for a software radio, because the resolution of the A/D fundamentally limits the radio's dynamic range.

This problem starts at the antenna. If a single antenna is used for both receive and transmit, then there is nothing to be done—we will always see the full transmit strength of the carrier that powers the tag.[2] It is possible to use two antennae, one for receive and one for transmit, and attempt to design these so that the receive antenna gets as little of the transmitted carrier as possible. At UHF or microwave frequencies, this is a particularly useful technique, because it is practical to construct a directional antenna. A similar approach can be taken at HF or LF: consider what happens if you have separate receive and transmit coils, at ninety degrees to each other (with the tag at 45 degrees to both of them).

Given a particular choice of antenna, this problem may now be addressed by analog signal processing in front of the A/D. Considering the problem in the frequency domain, it is obvious that what is needed is a tight notch filter at the carrier frequency—the $v_{tx}(t) = A_c \cos \omega_c t$ has energy at only one frequency, and we know that frequency exactly, because we are the ones (at the reader) generating it. As long the signal $v_{rx}(t)$ has no energy very close to ω_c (or as long as we can still demodulate $v_{rx}(t)$ after losing any components close to ω_c), the notch filter will not affect our information-bearing signal.[3]

[1] With some exceptions; for example, Motorola/Indala's FlexPass cards do BPSK on a 62.5 kHz subcarrier, with a 125 kHz carrier. I don't know of any 13.56 MHz standards that use wide modulation, though.

[2] Unless we try an isolator or other non-reciprocal device.

[3] And if $v_{rx}(t)$ did have important components near ω_c, then the situation would be hope-

(a) A ceramic or crystal filter is one practical implementation of this. The filter could either be applied directly, at the carrier frequency, or at at some IF after mixing the signal up or down. The frequency tolerance is tight enough that passive RLC, switched-capacitor, or active (R, C, and opamp) filters are not practical; but if the received signal is *(b)* mixed down by the carrier frequency, then the carrier is translated to DC, and the notch filter becomes a low-pass, which might be easier to implement. At that point only the dynamic range of the mixer is an issue, and that is likely an easier problem to solve.

(c) Equivalently, we could try to measure A_c, and add in

$$-A_c \cos \omega_c t$$

to try to cancel out the

$$A_c \cos \omega_c t$$

Even if we didn't do a perfect job, we would still be able to reduce the amplitude of the carrier term considerably, and perhaps reduce the dynamic range of the signal to the point that it was practical to handle it digitally from there on.

(d) Considering the problem in the time domain, the signal returned from the tag is an information-bearing subcarrier that amplitude-modulates the carrier. We wish to measure the amplitude of the received signal, which gives us

$$v_a(t) = A_c + v_s(t)$$

This is the subcarrier (that we want), plus a DC offset corresponding to the amplitude of the bled-through carrier. We can high-pass filter $v_a(t)$ with a very slow time constant to reject the DC offset, leaving only the subcarrier. It is necessary that $v_s(t)$ not carry any important information near DC, because those frequency components are rejected by the high-pass filter. This is equivalent to the previous requirement that $v_{rx}(t)$ not carry any important information near ω_c.

This device uses a single antenna for both receive and transmit, followed by a peak detector and simple analog filters. No frequency-domain attempt is made to reject our transmitted carrier. Since this device is intended as a test instrument, and not a long-range reader where the receiver sensitivity is critical, I consider this to be acceptable, but much better RF performance in the presence of noise (and our own transmitted carrier) could be achieved.

---

less, because A_c depends on a number of factors, including things like the proximity of metal objects to the reader.