Tufts University
School Of Engineering
Tufts Wireless Laboratory

Near-Field Identification of UHF RFIDs with WiFi

Zengxu Yang

April 9, 2019

Cross Technology Communication

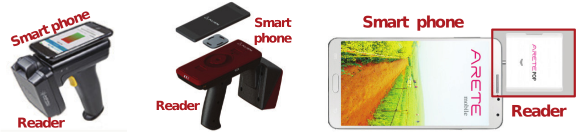
- Cross Techonlogy Communication (CTC) benefits cooperation among heteogenerous IoT devices.
- Most of the CTC systems work at the same frequency (eg. 2.4 GHz).
- The author develops a CTC system called TiFi that work with devices of different frequencies. The receivers (eg. WiFi enabled phones) works at 2.4 GHz can identify UHF RFID tags that work at around 800-900 MHz.

RFID, Pros and Cons

- Radio Frequency Identification (RFID) is increasingly used in day to day life because of the very low price of commercial RFID tags.
- A typical UHF RFID system works at about 800-900 MHz and a reader is needed.
- A UHF RFID tag does not need a battery and operates using the energy from signal emitted from the reader.
- RFID still cannot replace barcode in the consumer oriented market because typical mobile devices do not support it and special RFID readers are needed, unlike the barcode system.
- Some addon readers do not achieve wide adoption because of hardware cost and deployment complexity, thus cumbersome to use.

RFID Mobile Readers

They are either expensive, bulky, or inconvenient to use.



(a) TSL-1128 (b) ALR-S350

Figure 1: RFID Mobile Readers

RFID Readers and Their Limitations

Mobile Readers As mentioned before, they are either expensive, bulky, or inconvenient to use.

HTTP Readers Extremely expensive, limited to industrial usages.

Backscatters Modifications of the RFID tags are needed.

HF NFC NFC tags are more (20 times) expensive than RFID tags.

CTC and Its Limitations

- CTC allows cooperation of heterogenous technologies to cooperate, for example, ZigBee and WiFi. But they have to be at the same frequency.
- Because of the large different between the UHF RFID frequency (around 800-900 MHz) and WiFI frequency (2.4 GHz), no currently CTC system work for the cooperation of these two systems.

TiFi Introduction

- Tag emulated WiFi (TiFi) allows not only cooperation between different protocols but also different frequencies.
- TiFi allows a commercial WiFi receiver to identify a commercially available UHF RFID tag without modifying hardware or firmware.
- TiFi turns a tag into a virtual 802.11b WiFi AP that periodically broadcasts legitimate WiFi beacons that can be recognized by any WiFi receivers.
- Consumers identify RFID tags in the same way of identifying WiFi APs.

TiFi Architecture

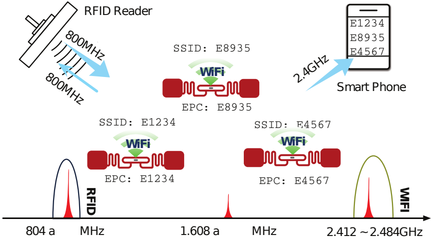


Figure 2: TiFi Architecture

How Does TiFi Work

- A RFID tag resonates the reader's continuous wave (CW) not only at the fundamental frequency (eg. 820 MHz) but at harmonic frequencies (eg. 1.64 GHz, 2.46 GHz, ...) too because of the nonlinearity of the retenna.
- TiFi utilizes the harmonic frequency near 2.4 GHz as the communication channel to communicate with WiFi receivers.
- The reader's continuous wave is crafted to create RFID Gen2 packets as well as WiFi 802.11b packets. The WiFi SSID is the Electronic Product Code (EPC).
- A prototype TiFi is created using the USRP N210 software radios.
- Experiments show that TiFi allows a commercial WiFi receiver to identify RFID tags within 2 m.

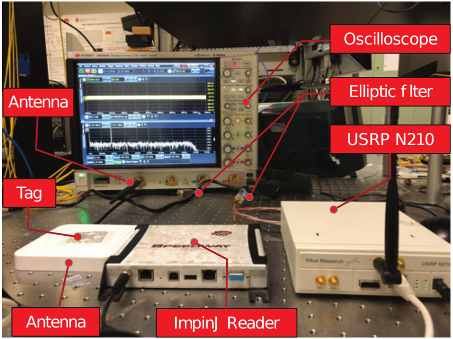
Frequncy Gap

RFID tags in different countries to different frequencies. The current RFID frequencies range from 840 MHz to 928 MHz. This means:

- The harmonic frequencies does not align well with the WiFi frequency. The desired fundamental frequency is around 820 MHz.
- Actually RFID tags have a wide resonation frequency range as wide as 300 MHz.
- To conform to regulations they only communicate with a narrow bandwidth of a few hundred kHz.
- A dual frequency CW is used to solve the frequency gap. One primary CW to support the EPC Gen2 protocol and a secondary CW for the backscattered WiFi.

Experimental Setup

Here is the experimental setup that uses a USRP N210 software radio as the TiFi reader, a commercial RFID reader for comparison, and a 4 GHz bandwidth oscilloscope to sniff backscattered signals.



USRP Setup

- The USRP N210 is used as the TiFi reader.
- GNU Radio on Linux is used to write and compile USRP code.
- The TiFi GNU Radio source code can be downloaded from `https://github.com/Anplus/TiFi`.