Enabling Ambient Backscatter Using a Low-Cost Software Defined Radio

Maximilian Stiefel
Uppsala University
maximilian.stiefel.8233@student.uu.se

Elmar van Rijnswou
Uppsala University
elmar.vanrijnswou.9818@student.uu.se

Carlos Pérez-Penichet
Uppsala University
carlos.penichet@it.uu.se

Ambuj Varshney
Uppsala University
ambuj.varshney@it.uu.se

Christian Rohner
Uppsala University
christian.rohner@it.uu.se

Thiemo Voigt
Uppsala University
and RISE SICS
thiemo@sics.se

***Abstract*—Backscatter communication is attractive for energy-constrained devices due to its very low power requirements. Ambient backscatter takes this point to the limit by leveraging existing radio frequency signals for the purpose of communication, without the need for generating an energy-expensive carrier signal. In this paper we investigate the use of television broadcast signals as a carrier for backscatter communication. As opposed to the state-of-the-art, restricted to operations under conditions of high signal strength, we demonstrate a low-cost software defined radio receiver that operates even in conditions when ambient signals are weak. We build the system using a low-cost off-the-shelf microcontroller and an RTLSDR software-defined radio receiver. We also conduct a survey of the signal strength of TV broadcast in a mid-sized Swedish city and observe that our system can operate in most parts of the city.**

I. Introduction

Backscatter enables wireless communication at orders of magnitude lower energy cost than traditional radios. A backscatter transmitter operates by either reflecting or absorbing existing wireless signals, which only incurrs in very low power consumption in the order of micro-Watts [1]. As a consequence backscatter communication is emerging as the mechanism of choice to network battery-free devices. Over the past few years significant progress has been made to make backscatter communication practical for Internet of Things (IoT) devices. Early backscatter systems, like RFID, required a dedicated device to generate the necessary carrier to be backscattered. State-of-the-art systems, however, reflect ambient WiFi or television signals [1] instead, which does away with the need for dedicated infrastructure.

Recent ambient backscatter systems demonstrate tag-to-tag communication by leveraging TV signals as a source of both carrier and energy. For example, Liu et al. present a proof-of-concept system that reflects ambient TV signals and enables tag-to-tag communication up to almost a meter. Parks et al. further improve the communication range to several meters by using analog coding [2]. While these systems can enable many applications, they are also restricted to operate only in environments where TV signals are fairly strong (approx $-30\,\mathrm{dBm}$) due to the low sensitivity of the receiver used in these tags. On the other hand, TV signals are known to vary greatly in strength [3] over space and time, making existing systems very restricted in their coverage.

On the other hand, Software Defined Radios (SDRs) are powerful devices that have significant processing abilities and offer relatively high receive sensitivity levels. The high sensitivity levels of the SDRs, compared to the typical ambient backscatter receiver tag, could significantly help improve the communication range and coverage when receiving ambient backscatter transmissions. More importantly, SDRs offer incomparable flexibility due to their ability to be reprogrammed. This flexibility offers the opportunity for ample experimentation, which is welcomed in this sort of emerging technology.

In this paper we explore the following questions: Can we create an SDR-based receiver for ambient backscatter transmissions? Can we leverage the relatively high sensitivity of such a receiver to improve range and coverage of ambient backscatter systems? Can we provide a flexible and low-cost experimentation platform for ambient backscatter research?

Contributions. The contributions of this work are twofold:

- We perform a survey of the signal strength of TV broandcast signals.
- We build a low-cost SDR-based receiver capable of receiving data encoded in backscatterer TV signals.

II. Background

In this section we introduce some necessary background related to our work.

A. Backscatter Transmissions

Consider an unmodulated carrier wave impinging on a backscatter tag's antenna. The signal observed by the receiver is:

$$S_r(t) = S_{rc}(t) + \sigma B(t) S_{bc}(t) \tag{1}$$

where $S_{rc}(t)$ is the signal coming directly from the carrier generator and $S_{bc}(t)$ is the signal from the carrier generator that reaches the backscatter tag. $B(t)$ is either zero or one and represents the instantaneous state of the backscatter tag: absorbing or reflecting, respectively.

Equation (1) reveals an important issue for backscatter communication systems: self-interference. The carrier signal $S_{rc}(t)$ interferes at the receiver with the data-carrying signal from the tag, $\sigma B(t) S_{bc}(t)$.

Recent work on generating backscatter transmissions has avoided self-interference through *frequency-shifted* backscatter [3], [4]. The tags modulate their antenna in such a way that their transmissions occur at a certain frequency offset from the carrier signal thus allowing the receiver to avoid interference from the carrier by tunning to the offset frequency where the tag is transmitting.

Consider the case when $B(t)$ periodically alternates between its two states at a frequency Δf while an unmodulated carrier of frequency f_c reaches the backscatter tag:

$$2\sin(f_c t)\sin(\Delta f t) = \cos[(f_c + \Delta f)t] - \cos[(f_c - \Delta f)t] \quad (2)$$

If we focus on only one of the two generated images, or employ single sideband backscatter [**?**], the data transmission can now be received at frequency $f_d = f_c + \Delta f$.

B. RTL2832U

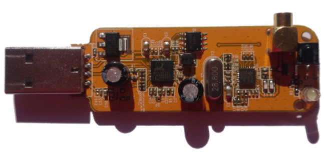

Fig. 1: *RTL-SDR* hardware with the DVB-T I/Q demodulator *Raeltek RTL2832U* (left IC) and the tuner with integrated LNA *Rafael Micro R820T/2* (right IC).

The *Realtek RTL2832U* is a terrestrial digital video broadcast (DVB-T) demodulator IC, which is the main part of a wide range of USB-based DVB-T receiver dongles. One prominent feature of this chip is that it allows to retrieve the raw I/Q samples via USB. This is originally intended for the chip to work as a simple DAB/FM software receiver. Ham radio enthusiasts have combined their efforts to create a software driver (the *librtlsdr*, cf. [5]) that allows DVB-T dongles based on the *RTL2832* to be converted into low-cost wideband SDR receivers. The cost of traditional SDRs has been in the range of a few hundred to thousands of USD. Albeit much less powerful than a typical SDR, a *RTL2832U*-based DVB-T receiver can be bought with antenna for less than 10 USD.

An RTL-SDR also contains a tuner that allows the user to select the received frequency. In our case the tuner is a *Rafael Micro R820T/2* which offers a tuning range from 42 to 1002 MHz [6]. Figure 2, shows a photograph of the RTL-SDR used in our work.

C. Quadrature Demodulation

The received signal can be interpreted as

$$s_{\mathrm{IF}}(t) = I(t) \cdot cos(\omega_0 t) + Q(t) \cdot sin(\omega_0 t) \quad (3)$$

This is multiplied with a cosine of the carrier frequency from a local oscillator.

$$\begin{aligned} s_{\mathrm{IF}}(t) \cdot s_{\mathrm{L}}(t) = I(t) \cdot cos(\omega_0 t) \cdot cos(\omega_0 t) \\ + Q(t) \cdot sin(\omega_0 t) \cdot cos(\omega_0 t) \end{aligned} \quad (4)$$

With $2\,cos(a)cos(b) = cos(a-b) + cos(a+b)$ and $2\,sin(a)cos(b) = sin(a+b) + sin(a-b)$ follows

$$\begin{aligned} 2 \cdot s_{\mathrm{IF}}(t) \cdot s_{\mathrm{L}}(t) = I(t) \cdot \big[1 + cos(2\omega_0 t)\big] \\ + Q(t) \cdot \big[sin(2\omega_0 t) + sin(0)\big]. \end{aligned} \quad (5)$$

One can see, that the interesting in-phase part (I) in this case is represented by a DC value after mixing. With a low-pass filter this DC value can be separated from the undesired rest. An analogous procedure is done with the quadrature part (Q) when mixing with a sine.

III. Design

In this section we describe the most important aspects of our design.

A. Transmitter

Our backscatter transmitter is designed to be used with the television signal, which has its center frequency at 626 MHz. To that end, we build an antenna using an unetched PCB plate as the ground plane and a wire that acts as the vertical antenna element.This antenna works well in the range from 626 to 245 MHz, which has been measured with a vector network analyzer (VNA).

Besides the antenna, the transmitter consists of an *MSP430* MCU, that sends data to the receiver. This transmitter controls an RF switch through an I/O pin. The switch can alternate the impedance connected to the antenna between matched (50 Ω) and open. The software now steers this switch with a two 2 MHz rectangular timer signal to transmit a data 1 or it just leaves the antenna open to transmit a data 0. Therefore the result is a frequency shift of the television signal by 2 MHz for a 1 and no shift for a 0. Hence a classical binary amplitude shift keying is the implemented modulation technique.

B. Receiver

We provide our C++ receiver code publicly available under [7] Figure 2 shows the architecture of our receiver, the signal flows from the left to the right. The raw I/Q data is available as two 8-bit values (real and imaginary) from the RTL-SDR. With these two values, the phase and magnitude of the data can be determined for every sample. The received signal can be represented as:

$$I + j\,Q = abs(I, Q) \cdot e^{j \times ang(I,Q)} \quad (6)$$

So the first block, entitled RTL2832U, provides the interface to the TV dongle. It controls the frequency f_{tuned}, where the receiver is listening as well as other interesting parameters e.g. the analog gain.

The demodulator block is responsible for converting the sampled signals into ones and zeroes. A FIR As part of the

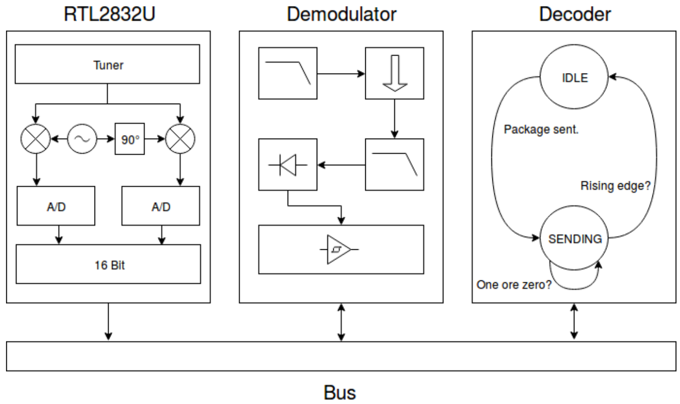

Fig. 2: Receiver architecture from a system point of view. Signal flow is from left to right.

demodulation process the signal is down-sampled and low-pass-filtered two times. The last demodulation step is to rectify the signal (cf. equation 7) and decide with a software-defined Schmitt trigger whether a sample is a 1 or a 0.

$$abs(I, Q) = \sqrt{I^2 + Q^2} \tag{7}$$

The resulting values are sent through the bus to the decoder. After the decoder received the samples it decides when a frame is sent or when the channel is idle. The decoder also includes a function to correlate the received bitstream with an expected pattern. Hence it is able to determine the bit error ratio (BER). Furthermore the code we have written so far subsumes different simulators for e.g. playing back recoreded data. Another handy utility, which has been written in Octave, is a tool (an oscilloscope) to look at the data, which is written into files by the demodulator. An example of a recorded data stream with 25 kS/s can be seen in figure 3.

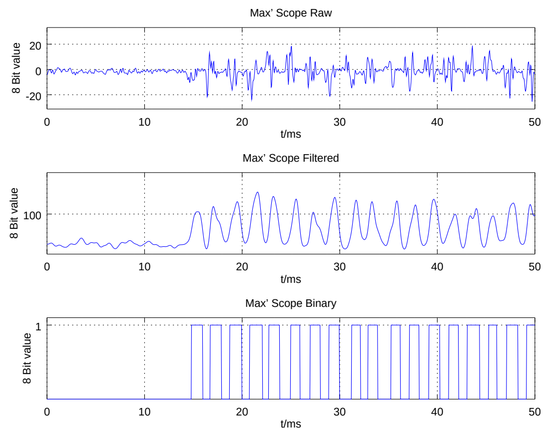

Fig. 3: Start of a transmission of 101010.. with 1 kbit/s with idle state before. Data from the Octave oscilloscope. Amplitude is quite low with an average of 12 % of the maximum, which is 127.5. This is due to a low signal strength. Sampling frequency is 25 kHz.

IV. Evaluation

In this section we present our evaluation results. The *RTL-SDR*, combined with intelligent signal processing in *Octave*, are the main tools we have employed for measurements.

A. Signal Strength Variation in Space

We have used the *RTL-SDR* to observe the space variations of the signal strength. *Octave* scripts have been written to aid in this purpose. These scripts are available under [8]. The scripts perform a frequency sweep through the desired band. The obtained samples are then transferred from the time domain to the frequency domain using a fast fourier transformation (FFT).

Because the RTL-SDR has a maximum (stable) sampling rate of 2.4 MS/s, we are limited to a maximum simultaneous acquisition band of 1.2 MHz. We keep a safety margin to the maximum capabilities and sample the desired frequency band at 900 kHz intervals and stitch these bands together to form the overall frequency sweep. This approach is valid only because we are not interested in real-time data. With this approach we are able to scan a 20 MHz band in roughly 30 seconds.

During the scanning process the gain is set to 40.2 dB. To get the signal strength we simply take the average over a 10 MHz band around the center frequency of the desired TV signal. This approach can be justified by the fact, that DVB-T is specified up to 10 MHz bandwidth. And the local TV provider advertises to be transmitting DVB-T 2. The signal $|H|$ is calculated as follows.

$$|H| = \left| \sum_{n=0}^{N} FFT\left(\Re\{s_{\text{band,n}}(t)\} \right) \right| \tag{8}$$

where N is the total number of intervals accumulated over the entire frequency sweep. The FFT is only carried out over the real values, which are received from the *RTL-SDR*. $s_{\text{band,n}}(t)$ is the signal in the time domain of one interval (one subband). There are as many samples taken in one band as needed for an FFT of size 2048. To finally get $|H_{tv,avg}|$ one has to normalize everything and calculate the power. Before doing that, a simple smoothing algorithm (FIR) is applied on $|H|$.

$$|H_{\text{tv,avg}}| = 20 \cdot log(|H|) - 20 \cdot log(|H_0|) \tag{9}$$

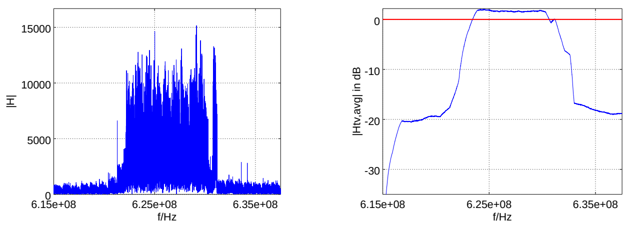

Fig. 4: Spectrum of the TV signal. Left: Raw spectrum of the TV signal with $f_{\text{center}} = 626$ Mhz. Right: Smoothed spectrum, normalized to maximum average measured in decibel with average shown as red line.

where $|H_0|$ is a normalization value measured at a certain point in space. The result of combining measured signal strength values with the haversine function to calculate the distance to the point where the maximum signal has been captured can be observed in figure 5.

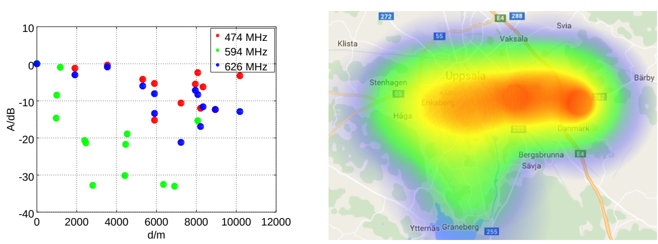

Fig. 5: Left: Signal strength fading against distance relative to the spot where the maximum signal strength has been captured (TV towers). 474 MHz and 626 MHz belong to a tower in Uppsala, Vedyxa and 594 MHz belongs to a tower in Uppsala, Rickomberga. Distances have been calculated with the Haversine formula. Right: Heatmap of the 626 MHz TV signal in Uppsala.

B. Communication Performance

We tested the communication with different data rates from 1 bit/s up to 1 kbit/s. As can be seen in Figure 3 the signal strength from the backscatter transmitter is rather low. This leads to a significant amount of quantization noise to appear. This situation can be improved by increasing the analog gain of the receiver. The transmission shown in figure 3 was carried out with the maximum gain (50 dB) available to our receiver.

With a data rate of 1 bit/s, we were able to achieve a range indoors of a couple of meters. With higher bitrates we can only communicate over a range of a few decimeters and the bit error rate is still approximately 40 %. The communication experiment was also carried out outside, close to the TV tower. We could not observe any improvements going closer to the tower.

V. Discussion

We are aware of the fact, that our communication system has to be improved until it is able to be used in allday technology. Different backscattering antennas have to be tried out to find the one with the best results. The question is mainly to which frequency the antenna has to be tuned (e.g. to the center of the TV signal or more to the edge of it). Moreover the standard *RTL-SDR* antenna including the coaxial cable are of quite low quality. The antenna is e.g. too short. Hence a custom antenna would be benificial at this point as well. Moreover some fine tuning can be made when it comes to the filter coefficients of the different filters. Finally the frame structure can be optimized to be able to correct errors (e.g. Hamming code).

To come to a conclusion one can say, that we were able to show, that spectrum scanning over a huge band with sweeping is possible using the *RTL-SDR*. Therupon we could provide a heat map of TV signals in a mid-sized swedish city as well as the tools to create it. And last but not least we have shown for the first time, that backscatter communication is possible with the *RTL-SDR*.

References

[1] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient Backscatter: Wireless Communication out of Thin Air," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, ser. SIGCOMM '13. New York, NY, USA: ACM, 2013, pp. 39–50. [Online]. Available: http://doi.acm.org/10.1145/2486001.2486015

[2] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging Ambient Backscatter Communication," in *Proceedings of the 2014 ACM Conference on SIGCOMM*, ser. SIGCOMM '14. New York, NY, USA: ACM, 2014, pp. 619–630. [Online]. Available: http://doi.acm.org/10.1145/2619239.2626312

[3] A. Wang, V. Iyer, V. Talla, J. Smith, and S. Gollakota, "FM Backscatter: Enabling Connected Cities and Smart Fabrics," 2017.

[4] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions," 2016, pp. 151–164. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/kellogg

[5] "steve-m/librtlsdr." [Online]. Available: https://github.com/steve-m/librtlsdr

[6] Rafael Micro, "High Performance Low Power Advanced Digital TV Silicon Tuner. R820t, Rev 1.2." [Online]. Available: http://www.rafaelmicro.com/product/view/21

[7] "s3xm3x/backscatterbaskreceiver." [Online]. Available: https://github.com/s3xm3x/backscatterBASKReceiver

[8] "s3xm3x/rtlsdrspecan." [Online]. Available: https://github.com/s3xm3x/RTLSDRspecAn