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 enables ultra-low power wireless transmissions, and is attractive for networking devices which operate on harvested energy. Ambient backscatter takes the concept further, by leveraging ambient wireless signals like television signals, as both the source of power and carrier signal. Existing state-of-the-art ambient backscatter systems demonstrate ability to achieve tag-to-tag communication under conditions when the strength of TV signals sufficiently high (-30 dBm). In this paper, we present our preliminary work which demonstrates the possibility to backscatter and communicate even when the ambient television signals are significantly weaker. The key to achieving this is to leverage a low-cost software defined radio receiver (RTLSDR) to receive backscattered transmissions. Our results demonstrate that the television signals are strong enough in most parts of a mid-sized swedish city for our system to operate, and communicate, a significant improvement over the state-of-the-art which are restricted to operate only when the tags are close to the TV towers.**

I. Introduction

Backscatter communication enables wireless transmissions at energy consumption which is several orders of magnitude lower than traditional radios. Backscatter achieves ultra-low power wireless transmissions by reflecting or absorbing ambient wireless signals, which as an operation consumes only μWs of power consumption [7]. As a consequence backscatter communication is emerging as the mechanism of choice to network devices operating on harvested energy. Over the past few years there has been significant progress to make backscatter a viable mechanism to network Internet of Things (IoT) devices. Traditional backscatter systems, like RFID readers, required a dedicated device to generate the necessary carrier signal reflected by the tags. On the other hand, state-of-the art systems does away the need for a dedicated device to generate carrier signals. Recent backscatter systems leverage already deployed infrastructure of devices to generate carrier signal [4], [10], or ambient WiFi [5], [12] or TV signals [7], [8].

Recent backscatter systems demonstrate ability to leverage existing signals like TV signals as a both source of 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 [8]. While these systems can enable many applications, these systems are severely restricted to operate in the vicinity of television towers where ambient signal are sufficiently strong (approx $-30\,\mathrm{dBm}$). This is primarily due to poor sensitivity levels of receivers employed on these devices, which together with weak backscatter reflections severely limits the operating range from the tower. On the other hand, TV signals are known to vary greatly in strength [11] both over space, and in time, which further aggravates the problem of limited range of ambient backscatter systems.

On the other hand, Software Defined Radios (SDRs) are powerful devices, and also have significant processing abilities. These devices offer high sensitivity levels, as compared to the receivers employed on typical ambient backscatter tags. Thus, SDRs might help to significantly improve the communication range, and also coverage area to receive ambient backscatter transmissions.

In this paper we explore the following questions: Can we leverage an SDR-based receiver to receive ambient backscatter transmissions ?, and, Does the relatively high sensitivity of SDR receivers improve range and coverage of ambient backscatter systems? A positive answer to the above question would provide a flexible and low-cost experimentation platform to the wider research community to explore ambient backscatter systems.

Contributions. In this paper, we make the following novel contributions:

- We design the first system which leverages a low-cost SDR to receive ambient-backscatter transmissions.
- Using the system designed, we demonstrate ambient backscatter using TV signals to be feasible in wide parts of a city. The range represents a significant improvement over the state-of-the-art.

The paper proceeds as follows. First, we discuss relevant background information of backscatter communication, SDR and reception process. Next, we present the design of the transmitter and the receiver employed in this paper. We then present initial results which evaluates our system. Finally, we present concluding remarks.

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:

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

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 [6], [10], [11]. 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 tuning 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

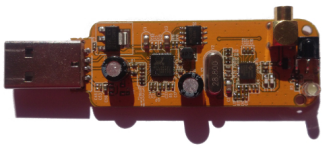

Fig. 1: *RTL-SDR* hardware with the DVB-T I/Q demodulator *Raeltek RTL2832U* (left IC) and the tuner with integrated LNA *Rafael Micro R820T/2* (right IC).

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. [3]) 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 [9]. 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.

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

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

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

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 design of our system. We first describe the design of the transmitter, next we describe the design of the receiver.

A. Transmitter

We design our backscatter transmitter to be used with ambient television signals. We design the transmitter for ambient television signal present in the band with center frequency of 626 MHz. Crucial to the design of the transmitter is the implementation of an antenna, as the antennas are known to be frequency selective. To this end, we design an antenna on an unetched board made of FR4 substrate commonly used to design PCBs. The board acts like the ground plane, at the center of the board we have a wire acting as a monopole antenna element. We have verified using a vector network analyzer (VNA), that the antenna can operate from frequency range most commonly used for television broadcast, from 245 MHz to 626 MHz.

Backscatter operates by reflecting or absorbing impinging radio signals on the antenna. To purposefully toggle the antenna to achieve these states, we terminate the antenna to a RF switch. The RF switch enables us to alternate the impedance connected to the antenna between matched (50 Ω) and open state. We control the RF switch through an I/O pin on a low-powered MCU, Texas instruments MSP430. As discussed earlier, to reduce the effects of self-interference, we frequency shift the backscatter transmission away from the TV signal.

Hence, we operate the RF switch using a 2 MHz intermediate frequency signal. Therefore the result is a frequency shift of the television signal by 2 MHz, when transmitting a bit 1, and no shift for a 0. Hence, we leverage amplitude modulation at receiver in our design. binary amplitude shift keying is the implemented modulation technique.

B. Receiver

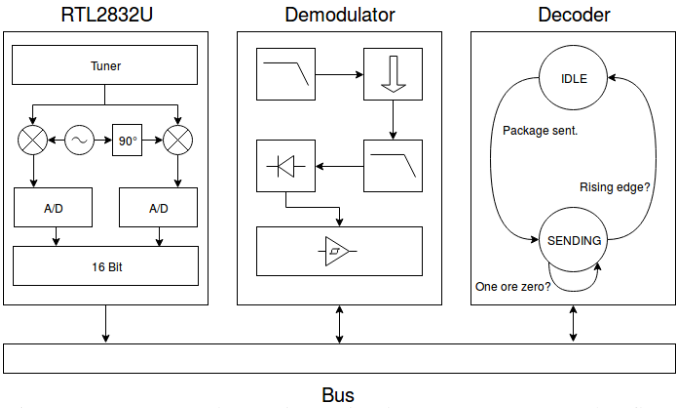

Fig. 2: *Design of the ambient backscatter receiver.* The flow of operation of the receiver is from the left to right.

The receiver consists of three main modules interconnected by a bus. The RTL-SDR block is in charge of collecting samples from the SDR-device. The demodulator turns the sampled signal into a streams of ones and zeroes. Finally, the Decoder block is in charge of detecting frames. We provide our C++ receiver code publicly available under [1].

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:

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

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. As part of the 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 recorded 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.

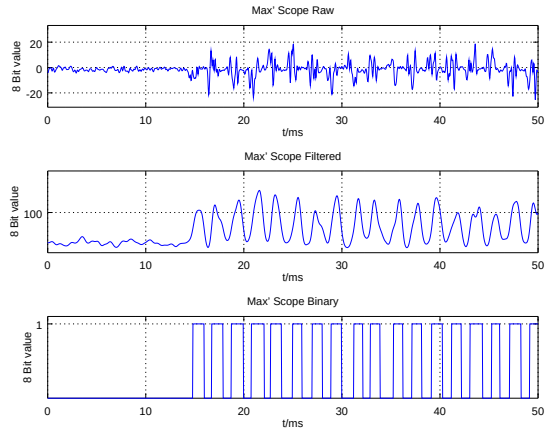

Fig. 3: Start of a transmission of 101010.. with 1 kbit/s with idle state before. Data from the Octave oscilloscope. Amplitude is quite low with an average of 12 % of the maximum, which is 127.5. This is due to a low signal strength. Sampling frequency is 25 kHz.

IV. Evaluation

In this section, we present the results of evaluation of our system. As experimental setup, we use RTLSDR together with signal processing algorithm implemented in Octave.

A. Spatial variation of ambient television signals

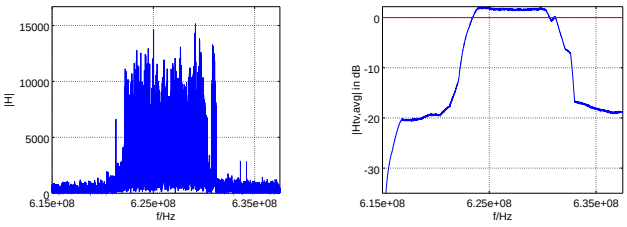

Fig. 4: *Observed spectrum of television signal.* The left hand image shows the raw spectrum of the TV signal, with centre frequency of 626 MHz. The right hand image shows the smoothed spectrum normalized to maximum average. The average is shown by the horizontal red line.

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 [2]. 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 $|H|$.

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

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.

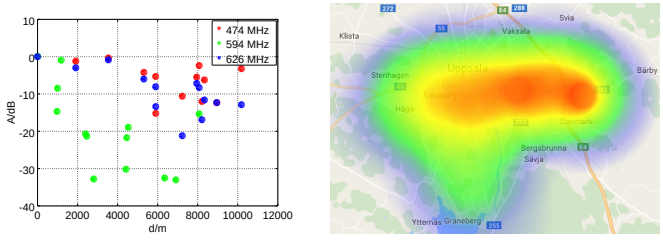

Fig. 5: Left: Signal strength fading against distance relative to the spot where the maximum signal strength has been captured (TV towers). 474 MHz and 626 MHz belong to a tower in Uppsala, Vedyxa and 594 MHz belongs to a tower in Uppsala, Rickomberga. Distances have been calculated with the Haversine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

V. Discussion

Our system still has a lot of room for improvement. Different backscattering antennas could be tried to find the one with the best combination of gain, tuning frequency and bandwidth. Moreover the standard *RTL-SDR* antenna and its coaxial cable are of low quality. Hence a custom antenna would be beneficial. Furthermore some fine tuning can be made when it comes to the filter coefficients of the different filters in the demodulator chain. Finally errors can be further reduced by using one of many available forward error correcting codes.

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*. This allowed us to perform a survey of the TV signal strength in the city. And finally we have shown for the first time, that backscatter communication is possible with the *RTL-SDR*.

References

[1] s3xm3x/backscatterbaskreceiver.

[2] s3xm3x/rtlsdrspecan.

[3] steve-m/librtlsdr.

[4] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*, pages 356–369. ACM, 2016.

[5] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. *ACM SIGCOMM Computer Communication Review*, 44(4):607–618, 2015.

[6] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. pages 151–164, 2016.

[7] 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*, SIGCOMM '13, pages 39–50, New York, NY, USA, 2013. ACM.

[8] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith. Turbocharging Ambient Backscatter Communication. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, pages 619–630, New York, NY, USA, 2014. ACM.

[9] Rafael Micro. High Performance Low Power Advanced Digital TV Silicon Tuner. R820t, Rev 1.2.

[10] A. Varshney, O. Harms, C. P. Penichet, C. Rohner, F. Hermans, and T. Voigt. Lorea: A backscatter reader for everyone! *arXiv preprint arXiv:1611.00096*, 2016.

[11] A. Wang, V. Iyer, V. Talla, J. R. Smith, and S. Gollakota. Fm backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, pages 243–258, Boston, MA, 2017. USENIX Association.

[12] P. Zhang, D. Bharadia, K. Joshi, and S. Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, SenSys '16, pages 259–271, New York, NY, USA, 2016. ACM.