Enabling Backscatter Communication among Commodity WiFi Radios

Pengyu Zhang[1*], Dinesh Bharadia[2*], Kiran Joshi[1], Sachin Katti[1]
Stanford University[1], MIT[2]
Co-primary Student Authors[*]
{pyzhang, krjoshi, skatti}@stanford.edu, dineshb@csail.mit.edu

ABSTRACT

We present the first low power backscatter system that can be deployed completely using commodity WiFi infrastructure. With this system, a low power tag reflects existing 802.11b transmissions from a commodity WiFi transmitter, and the backscattered signals can be decoded as a standard WiFi packet by a commodity 802.11b receiver. The key invention is a novel technique called **codeword translation**, which allows a backscatter tag to embed its information on standard 802.11b packets by just translating the original transmitted 802.11b codeword to another valid 802.11b codeword. This allows any 802.11b receiver to decode the backscattered packet, thus opening the doors for widespread deployment of low-power backscatter communication using widely available WiFi infrastructure. We show experimentally that we can achieve an uplink throughput of up to 1Mbps at ranges of up to 8m and ranges of up to 50m where it achieves a throughput of around 100Kbps, which is twice as better than the recently published passive WiFi system.

CCS Concepts

•Networks → Network architectures; Wireless access networks;

Keywords

Backscatter; Sensor; Wireless

1. INTRODUCTION

Backscatter communication has recently attracted interest for applications such as implantable sensors, wearables, and smart home sensing because of its ability to offer near zero-power connecitivity to these sensors. These applications have severe power constraints, implantable sensors for example have to last for decades, while even more traditional smart home monitoring applications will benefit from sensors and actuators that can last several years. Backscatter communication can satisfy the connectivity requirements while consuming so little power that it could be powered by harvesting alone, or with batteries that could last several years.

Current backscatter systems however require specialized hardware to generate the excitation RF signals that backscatter radios can reflect, as well as to decode the backscattered signals. Recent research such as passive WiFi [1] has reduced the need for specialized hardware. Passive WiFi for example can decode using standard WiFi radios, however it still requires a dedicated continuous wave signal generator as the excitation RF signal source. BackFi needs a proprietary full duplex hardware add-on to WiFi radios to enable backscatter communication. Consequently, a backscatter system that can be deployed using commodity devices such as access points, smartphones, watches and tablets does not exist.

Further, recent work such as Passive WiFi also requires twice the spectrum compared to other approaches such as BackFi, since they generate the RF excitation tone signal on the center of two WiFi channels and the backscatter tag frequency shifts and reflects the excitation signal on both the adjacent WiFi channels. Due to the frequency shifting, the WiFi device (the reader) thats decoding the backscattered signal does not need full duplex hardware. However the tradeoff is that for a single backscatter communication link, we end up using two 20Mhz WiFi channels. For example, the continuous wave signal generator send outs a tone at the center of Channel 3 and the backscatter occupies both Channel 1 and 6, rendering them unusable for any other WiFi communication. Given the paucity of spectrum in the unlicensed band, solutions that do not waste spectrum would be desirable.

We introduce the first backscatter communication system that works using only commodity 802.11b WiFi devices for both generating the RF excitation signal as well as decoding the backscattered signal. We observe that most users are surrounded by multiple WiFi radios, either in APs or on their phones and tablets or even on their smartwatches. Our

SIGCOMM '16, August 22-26, 2016, Florianopolis , Brazil

DOI: http://dx.doi.org/10.1145/2934872.2959072

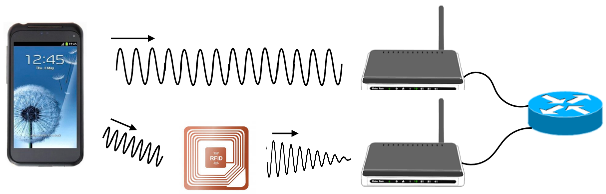

Figure 1: Our system concept: our system enables backscatter communication between commodity 802.11b WiFi radios.

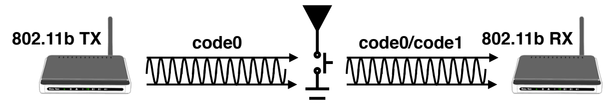

Figure 2: 802.11b code word translator at the tag.

system reuses these commodity WiFi radios as both an RF source for backscatter as well as to receive the backscattered signals. This allows our system to be very cost effective and widely deployable since it can benefit from the tremendous ubiquity and low-cost nature of WiFi and eliminate the need for a specialized, dedicated reader or receiver. Second, our system does not waste spectrum, it piggybacks backscattered signals on WiFi packets that are being used for productive communication. Hence our system can be efficiently deployed with current WiFi infrastructure and unlicensed spectrum.

The deployment of our system is best explained via the example in Figure 1. The excitation device is a smartphone with a standard WiFi radio. The smartphone transmits a 802.11b packet to the first AP to which it is connected on Channel 1. To backscatter, the tag receives the WiFi packet, frequency shifts it to Channel 6, modulates its information and then reflects the WiFi signal. The second AP, which is tuned to listen on Channel 6, then receives and decodes the backscatter packet as a standard WiFi packet. Thats the entire operation of our system, it does not need any specialized hardware nor does it waste any spectrum, both WiFi channels are used for productive communication, one for standard WiFi and the other for the backscatter link.

The key challenge in realizing our system is: how can a backscatter tag produce a WiFi compliant packet by backscattering another WiFi compliant packet and also modulate its data on the resulting packet? The key conceptual contribution here is **codeword translation**. Specifically, every 802.11b WiFi packet is a sequence of codewords that are picked from a codebook to represent different bits that are being transmitted. In our system, backscatter tags act as codeword translators, in other words they take a valid codeword in the transmitted 802.11b packet and translate it into a different valid codeword from the 802.11b codebook. The specific translation encodes the bit that the backscatter tag itself wants to communicate. The backscattered packet is therefore like any other 802.11b packet, albeit with a sequence of translated codewords depending on the data that backscatter tag wants to communicate. Consequently it can be decoded by any standard 802.11b receiver.

2. DESIGN

Figure 2 shows an overview of our system. A commodity WiFi radio transmits a normal 802.11b WiFi packet, the backscatter tag reflects the packet to another 802.11b WiFi radio while modulating its information. When the tag backscatters the packet, it shifts the frequency of the reflected signal to an adjacent WiFi channel. The 802.11b receiver listening on the adjacent WiFi channel receives the reflected WiFi packet, decodes the packet using the normal WiFi decoding chain, and then extracts the backscattered information from the decoded bit stream.

The key idea underlying our system is the concept of codeword translation. Conceptually, any modulation scheme (including WiFi's) is a mapping between bits and codewords from a discrete codebook. Decoding is the inverse operation, mapping from a received codeword to the actual bit. For a commodity WiFi receiver to decode the backscattered packet, its codewords need to come from the same codebook as WiFi's. In other words, if the backscatter tag can act as a **codeword translator**, i.e. translate the codewords from the original 802.11b packet to other codewords in the 802.11b codebook, then a standard 802.11b receiver will be able to decode the packet, and a standard 802.11b transmitter can transmit original data. For example, equation 1 shows how the codeword for 1 and codeword for 0 are related, or in otherwords codeword 0 can be translated into codeword 1. The trick of course is to implement the translation based on what bits the tag wants to backscatter and such that the 802.11b receiver can recover the applied translation and therefore recover what bits the backscatter tag wanted to communicate.

$$\begin{aligned} &\text{codeword } 0 = 1 \times \text{barker} \\ &\text{codeword } 1 = -1 \times \text{barker} = \text{codeword } 0 \times e^{j\pi} \end{aligned} \tag{1}$$

For backscattering 802.11b 1Mbps signals, FS-Backscatter's tag implements a simple translation. If it wants to backscatter the bit zero, then it does no translation and simply reflects the original codeword. If it wants to backscatter bit one, then it translates the received codeword to the only other valid codeword in the 802.11b 1Mbps codebook. To do so, it simply shifts the phase of the received codeword by 180 degrees as show in equation 2. If the original 802.11b bit was zero, this will translate to a one being backscattered, and vice versa if the original 802.11b bit was one. This is shown via equation 2. Figure 2 shows an example of such translation.

$$\begin{aligned} &\text{Tag data } 0 = 802.11\text{b data} \\ &\text{Tag data } 1 = 802.11\text{b data} \times e^{j\pi} \end{aligned} \tag{2}$$

Acknowledgement

This research was partially funded by the gift from Huawei and Deutsche Telekom.

3. REFERENCES

[1] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith. Passive wi-fi: bringing low power to wi-fi transmissions. In *NSDI*, 2016.