Augmenting IoT Networks with Backscatter-Enabled Passive Sensor Tags

Carlos Pérez-Penichet[1], Frederik Hermans[1], Ambuj Varshney[1], Thiemo Voigt[1,2]

[1]Uppsala University, Sweden [2]SICS Swedish ICT

ABSTRACT

The sensing modalities available in an Internet-of-Things (IoT) network are usually fixed before deployment, when the operator selects a suitable IoT platform. Retrofitting a deployment with additional sensors can be cumbersome, because it requires either modifying the deployed hardware or adding new devices that then have to be maintained. In this paper, we present our vision and work towards *passive sensor tags*: battery-free devices that allow to augment existing IoT deployments with additional sensing capabilities without the need to modify the existing deployment. Our passive sensor tags use backscatter transmissions to communicate with the deployed network. Crucially, they do this in a way that is compatible with the deployed network's radio protocol, and without the need for additional infrastructure. We present an FPGA-based prototype of a passive sensor tag that can communicate with unmodified 802.15.4 IoT devices. Our initial experiments with the prototype support the feasibility of our approach. We also lay out the next steps towards fully realizing the vision of passive sensor tags.

CCS Concepts

•**Networks** → **Network architectures; Wireless access networks;**

Keywords

Backscatter communication, Internet of Things, Wireless

1. INTRODUCTION

The Internet of Things (IoT) is expected to bridge the physical world and the digital world by instrumenting the former with sensors and actuators. With millions of devices installed, repurposing an existing sensing application—or simply adding new sensing capabilities—can be a daunting task. We introduce *passive sensor tags*, battery-free devices to augment existing IoT deployments by collecting and transmitting their readings to nearby active devices without requiring any modification to the deployed hardware.

HotWireless'16, October 03-07, 2016, New York City, NY, USA

DOI: http://dx.doi.org/10.1145/2980115.2980132

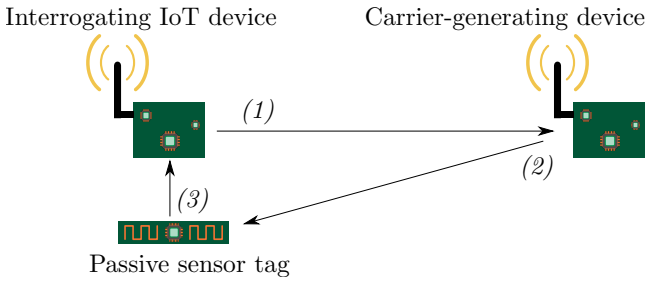


Figure 1: **Passive sensor tags add new sensing capabilities to commodity IoT devices in their vicinity.** To query a passive sensor tag, a device requests one of its neighbors to generate an unmodulated carrier (1), which reaches the tag (2). The tag modulates the carrier with a valid 802.15.4 packet to the requesting device (3).

In our vision (Figure 1), an IoT network can be augmented with a new sensor by simply placing a passive sensor tag with the desired capability next to one of the deployed devices. We envision passive sensor tags to have the form factor of a sticker, similar to today's RFID tags. Deploying a passive sensor tag would be as simple as placing them next to an already deployed device. There would be no need to change the deployed hardware nor to add new communication capabilities or power sources. Instead, a deployed active device queries a nearby passive sensor tag by requesting a neighboring device to generate an unmodulated carrier. The passive sensor tag then transmits its reading using backscatter communication, essentially modulating the carrier "in the air". The resulting packet can be seamlessly received by the querying device.

Passive tags are based on the principle of backscatter communication and build on recent research that creates passive transmissions of popular wireless communication standards like Bluetooth LE [12] and WiFi [15]. Our contributions differentiate our work from those in three key aspects:

1. Our system does not require the use of an additional external device to generate the unmodulated carrier. Instead, we rely on the radio test mode present in many IoT radio transceivers to generate an unmodulated carrier necessary for backscatter transmissions.

2. We employ IEEE 802.15.4, a popular protocol in existing commodity IoT network deployments, thus bridging

the gap for those networks to leverage ultra-low-power communication with ease.

3. We focus on the idea of augmenting an existing sensing network deployment with new sensing capabilities without the need for any modification to the deployed devices.

We have implemented a prototype of a passive sensor tag using an FPGA. The prototype is able to generate 802.15.4 packets, a protocol commonly employed by commodity IoT devices. Using the prototype, we performed a set of experiments that constitute a first step to show the feasibility of our vision.

Our experimental results indicate that a passive sensor tag can reliably transmit its readings to active devices up to an approximate distance of 20 cm. Crucially, our results are obtained without the need for an ad-hoc device to generate the necessary unmodulated carrier, relying on the IoT devices to provide this function instead.

2. TRANSMITTING 802.15.4 PACKETS WITH BACKSCATTER

In this section, we present a brief overview of the fundamental aspects that make our vision possible and introduce our working prototype of a passive sensor tag.

A backscatter transmitter works by absorbing or reflecting existing radio frequency signals. The transmitter modulates its antenna's radar cross section by toggling a switch across the antenna terminals. The radar cross-section changes cause variations in the existing signal that can be used to decode transmitted information when observed by the receiver.

The backscattered signal observed at the receiver is proportional to the product of the signal reaching the backscatter antenna and the signal driving the switch [16], which is our baseband signal. Considering the case of a sinusoidal carrier of frequency f_c and a switch driven at a frequency Δf the resulting product is

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

This shows how the product results in two frequency-shifted images of the original carrier. The resulting images are shifted up and down the frequency spectrum by an amount equal to the frequency of the baseband signal. Our passive tags leverage this displacement—or mixing—property to avoid interference from the unmodulated carrier. This is achieved by shifting the baseband signal away from the carrier frequency. Because the phase of the baseband signal is preserved in this process, it is possible to modulate the resulting images using any kind of phase modulation.

The IEEE 802.15.4 standard for low-rate wireless personal area networks [8] defines the channel assignment and modulations used by this class of networks. The standard specifies 16 channels spaced every 5 MHz in the 2.4 GHz ISM band. For transmissions in this band, the standard mandates a physical layer that uses direct sequence spread spectrum (DSSS) with offset quadrature phase shift keying (O-QPSK) modulation. Data is transmitted at an effective rate of 250 kbps.

A transmitter works as follows: Initially the data is split into groups of 4-bits. To increase robustness, each group is encoded into one of 16 predefined chip sequences of length 32. The resulting chips are subsequently modulated using O-QPSK and are then transmitted.

The O-QPSK modulator encodes two chips per symbol in a set of four possible symbols. Each one of them is represented by a sinusoidal signal with a pre-specified phase offset. One way of generating an O-QPSK modulated signal is to switch the phase offset of a constant-amplitude carrier according to the desired symbol. This is what our prototype does.

Our passive sensor tag prototype is capable of transmitting arbitrary 802.15.4 packets. The prototype is based on the DE0-nano FPGA development board from TerasIC [6] which features an Altera Cyclone IV FPGA. In the FPGA, we implemented all the baseband logic to generate 802.15.4 frames for an arbitrary payload. The prototype also modulates the generated baseband signal with an intermediate frequency of Δf=10 MHz and makes the resulting signal available through an output pin. Whenever the modulated signal is positive, the output pin is set high, otherwise it is set low. This signal, in turn, drives the base of an RF transistor switch (BFT25A) connected across the antenna terminals. Whenever the pin is high, the switch is closed and the antenna is short-circuited, causing incident RF to be reflected. Conversely when the pin is low, the switch is open and incident radio waves are absorbed. In this way, the payload is modulated on the incident carrier. Note that, while the FPGA prototype itself has a relatively high power consumption, an equivalent ASIC implementation would have a power consumption in the order of a few microwatts, making it comparable to other current backscatter transmitters [15].

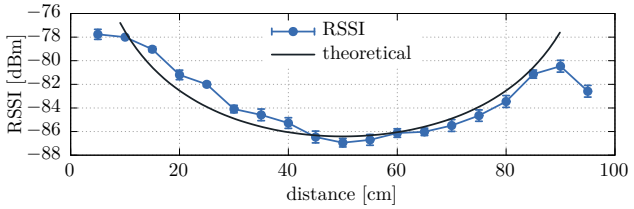
3. RECEIVING PASSIVE 802.15.4 PACKETS

In this section we present experimental results that illustrate how our vision is possible. We begin investigating the achievable communication range, as well as how the packet reception rate changes with distance to the receiver. Next we look into the selection of an appropriate value of Δf, and finally assess the carrier strength that can be achieved from other IoT devices using the radio test mode.

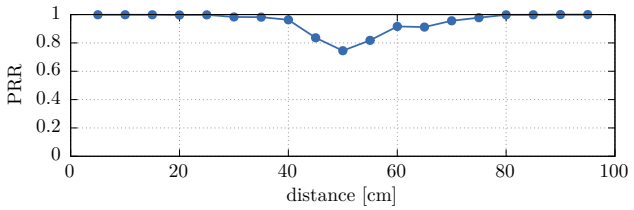
3.1 Impact of distance

An essential question when assessing the feasibility of our vision is: how close to the receiving node does a passive sensor tag need to be for successful operation?

In this experiment we placed two commodity IoT devices (TelosB motes [7]) one meter apart from each other. One of the IoT devices generated a constant carrier at a nominal transmit power of 0 dBm, while the other acted as a receiver. The carrier was transmitted on channel 19 ($f_c = 2.445$ GHz) while the receiver was tuned to channel 21 ($\Delta f = 10$ MHz). We moved our transmitter prototype along the line from the receiver (located at position 0 cm) to the carrier generator (at position 100 cm) at 5 cm intervals . At each position, the passive tag transmitted 1000 packets with random payloads of 12 byte each, while the receiver recorded all received packets. We then compute the Packet Reception Rate (PRR) for every position. Additionally, at every step, the receiver node measured the signal strength (RSSI) for 30 seconds, while the prototype generated an intermediate frequency carrier of frequency $\Delta f = 10$ MHz. This allows the receiver to know the signal strength on the reception channel for every position of the passive sensor tag. The experiment was performed inside an anechoic chamber to discard any effects caused by multipath propagation and interference.



(a) **Average RSSI.** The error bars represent the standard deviation.There is great correspondence between the experimental results and expected theoretical behavior.



(b) **PRR.** Packet losses only appear for distances larger than 20 cm from the receiver or the carrier generator

Figure 2: **Receiver-sender distance dependencies.** The receiver is at position 0 cm and the transmitter at 100 cm. The carrier is transmitted at 0 dBm.

Figure 2a shows the resulting curve for average RSSI as a function of the distance between the receiver and the passive sensor tag. Error bars represent the standard deviation. The graph displays the expected bathtub shape and matches very well with the theoretical radar range equation curve [9]. This result shows how the optimal location for our tag is close to one of the two nodes, either the one generating the carrier or close to the receiver. Signal strength is relatively poor at intermediate locations, which should thus be avoided.

Figure 2b presents the results for the measurement of PRR as a function of distance. The curve unsurprisingly mimics the valley of Figure 2a: as signal strength is lower for the intermediate positions, so is PRR. This result suggest that for distances up to 20 cm, the reception rate should be sufficiently high. This fact is encouraging, considering that in our vision passive sensor tags would generally be located close to the receiving IoT device. A range of 20 cm is reasonable once we consider the carrier strength in our scenario is roughly 30 dB lower than in other work [15].

3.2 Impact of Δf

As mentioned in Section 2, our tags avoid interference from the unmodulated carrier by introducing a frequency difference Δf between the generated 802.15.4 frames and the carrier. We briefly present experimental results to answer the question of what is the optimal value of Δf.

The optimal value of Δf is determined by two factors. On one hand, the unmodulated carrier should be far enough from the receiving channel so that it does not interference on the receiver. On the other hand, Δf should be as small as possible for lower power consumption and simplicity of the electronics design of the passive sensor tags. With these two requirements in mind, the smallest value of Δf that is attenuated enough by the receiver will be the optimal value. In other words, this aspect is controlled by the selectivity of the receiving device. The higher the selectivity, the more

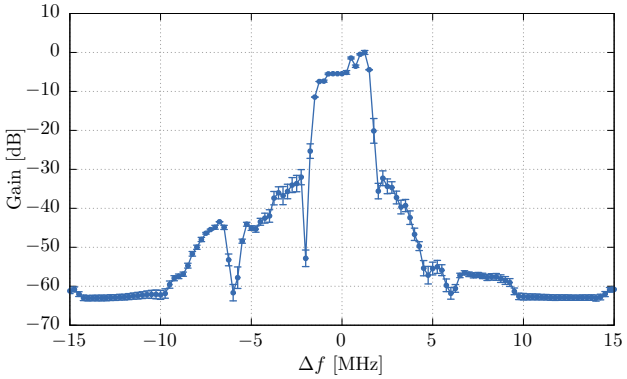


Figure 3: **Normalized average carrier rejection as a function of Δf.** The error bars represent the standard deviation. For the best results Δf should be set at least to 10 MHz.

rejection the receiver presents to an interfering signal on a nearby channel.

The IEEE 802.15.4 [8] standard mandates a minimum adjacent channel rejection of 0 dB and a minimum alternate channel rejection of 30 dB. The specific case of the CC2420 [3], a widely used 802.15.4 radio transceiver, presents an adjacent channel rejection of at least 30 dB and an alternate channel rejection larger than 50 dB. Equivalent transceivers from other manufacturers [1, 2, 4, 5] present similar or better figures. With these values in mind, it seems possible to transmit the carrier in one channel and receive the data on the alternate channel (two channels away) using $\Delta f = 10$ MHz. We have performed a simple experiment to corroborate this.

The experiment consists of an IoT device—a TelosB mote, which features a CC2420 transceiver—tuned to a fixed channel (channel 21, $f_R = 2.455$ GHz). In this case an unmodulated carrier was generated with a B200 Software Defined Radio (SDR) from Ettus Research for fine-grained frequency control. The constant carrier was transmitted at a frequency $f_R + \Delta f$, where f_R is the nominal frequency of the receiving channel. The receiving IoT device was set to measure the signal strength for 30 seconds at a time as the value of Δf was changed. This experiment was also performed inside an anechoic chamber.

Figure 3 shows the average signal rejection as a function of Δf. The error bars represent the standard deviation. The figure clearly shows that the measurements largely agree with the values in the transceiver's specification. Using $\Delta f = 5$ MHz (corresponding to one 802.15.4 channel) is not optimal. Instead, a much better rejection is achieved by setting $\Delta f \geq 10$ MHz. We have chosen $\Delta f = 10$ MHz (two 802.15.4 channels away) for all our experiments.

3.3 Characterizing Carrier Strength in a Deployed Network

Our idea builds on the premise that a node can query a passive sensor tag by requesting a neighbor to generate an appropriate carrier. Many IoT transceivers have a radio test mode able to transmit an unmodulated carrier. Even if this mode is intended for regulatory certification, we propose to use it for carrier generation. An important consideration in this context is the achievable carrier strength, because IoT

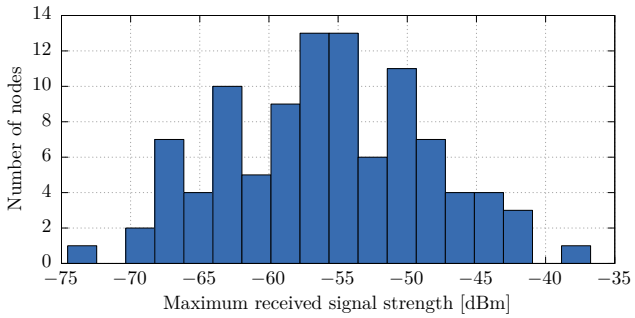


Figure 4: **Distribution of maximum signal strength from neighbors.** Assuming a return loss of less than 10 dB at the passive tag, all nodes have at least one neighbor that can supply a carrier of sufficient strength.

devices are usually limited in their output power. Will the carrier from a neighboring node be strong enough for the querying node to receive backscattered packets?

For an initial exploration of this question we ran an experiment on Indriya [11], an IoT testbed at the National University of Singapore. The testbed consists of 100 commodity IoT devices that are deployed over three floors. In the experiment, nodes continuously listen for packets and log the signal strength of any received packet. Meanwhile, nodes transmit packets at random intervals. Note that because the amplitude of an O-QPSK-modulated signal is constant, the signal strength of a received packet is a good indication of the strength of a carrier emitted by the sending node.

Figure 4 shows the distribution of the maximum signal strength that each node observed from all its neighbors. We have to account for an additional return loss that is incurred at the passive tag. Kellogg et al. report a return loss of 1.1 dB [15]. Under the assumption that we can optimize our prototype to have a comparably low return loss, all nodes in the experiment would have at least one neighbor they can rely on to generate a carrier.

Although this initial experiment is too limited to draw strong conclusions, the results nonetheless suggest that leveraging nearby nodes to generate a carrier in existing IoT deployments may be a feasible approach to integrating passive sensor tags.

4. NEXT STEPS

Before our passive tag vision can be fully realized, we need to address a number of system and protocol challenges. These are subject of our ongoing work, and we briefly discuss them here.

In the current state, our tags have no medium access control abilities. The tags simply transmit their readings whenever a carrier is available. In a low-density network in which there are only few passive tags, medium access may not be necessary due to the tags' limited transmission range. However, as the network size and the number of tags increases, the problem needs to be handled more explicitly.

Our tags currently lack reception capability, and therefore cannot use carrier sense to avoid collisions. For deployments in which there are only a few sensor tags for each node, we are considering a simple random backoff scheme. The likelihood of collision between tags is further reduced when the passive sensor tags are powered from the RF carrier, as they are likely to wake up at different times due to varying length of the charging process. We are also investigating how we can add reception capabilities to the passive sensor tags, so that we can implement more advanced medium access control.

When a node generates a carrier to enable nearby passive sensor tags to transmit, the carrier can interfere with other transmissions in the channel that corresponds to the carrier's frequency. To avoid disruptions from carrier generation, our first step is to assume a protocol such as Glossy [13] in the deployed network. With Glossy, the network will be tightly time-synchronized and specific time slots can be dedicated to generating carriers and querying nearby passive sensor tags. In this way, we can avoid interference between existing traffic and transmissions from the passive sensor tags or the carriers. We will later look into more dynamic protocols for querying the tags.

In a scenario where many different networks are co-deployed, it may be an issue that the passive tag transmissions occupy three channels instead of just one (one channel is occupied by the carrier and two channels are occupied by the reflected signals). Even though the backscatter transmissions are limited in space, the issue requires further study.

Finally, since we envision passive tags to be easily-deployable stickers that operate on harvested energy, we expect the low power availability to put some constraints on the type of sensors we can employ. There is however, a large variety of micro-power sensors of many kinds that consume power in the range of a few microwatts [21]. These would be suitable for even the most stringent of conditions.

5. RELATED WORK

Backscatter communication has been extensively researched, primarily in relation to RFID devices. However there have been recent efforts to network sensors and IoT devices using backscatter communication.

Zhang et al. argue that communication is more energy consuming than computation in backscatter devices, and thus stream raw data from sensors and avoid local computation [21]. WISP [19] and Moo [20] are computational RFID platforms that allow interfacing of external sensors and use backscatter communication. Talla et al. build on WISP and propose analog backscatter to stream audio signals [18]. Likewise, Naderiparizi et al. demonstrate a battery-free camera that uses backscatter communication [17].

Unlike these prior works, our work does not rely on an RFID reader to query the sensors. Furthermore, we do not focus on a specific sensing modality, but explore passive sensor tags as a new component in existing IoT architectures.

Ambient backscatter leverages ambient RF signals such as TV transmissions [16] or WiFi traffic [10, 14] to dispense with the need for an external reader. Parks et al. demonstrate passive tag-to-tag communication using ambient TV signals [16]. Kellogg et al. demonstrate the feasibility of backscattering WiFi signals and receiving on commodity smart phones [14]. Bharadia et al. demonstrate high throughput backscatter with WiFi signals [10]. Our present work is complementary to these efforts; however, passive sensor tags could also leverage ambient RF signals.

More recent efforts focus on receiving backscatter transmissions using commodity radio chips [12, 14, 15]. Kellogg et al. create IEEE 802.11b packets using backscatter and receive the packets on WiFi chipsets [15]. Ensworth et al. gener-

ate Bluetooth Low Energy (BLE) packets using backscatter communication [12]. Our work is similar to these efforts in that we also use backscatter communication to implement an existing, widely deployed wireless protocol. However, we focus on bringing the benefits of backscatter to existing 802.15.4 deployments that might otherwise not benefit from passive WiFi and similar efforts. More crucially, our work differs from the mentioned work in that we do not rely on external infrastructure to generate a suitable carrier. Instead, we leverage capabilities that are available in deployed IoT devices.

6. CONCLUSION

In this paper, we have reported on our first steps towards our vision of augmenting the sensing capabilities of deployed IoT networks using passive sensor tags. Our experiments suggest that our vision is realizable.

We showed that transmissions from passive sensor tags can be received at distances of up to ca. 20 cm. Since we expect passive sensor tags to be devices with very a small form factor that are placed close to a commodity IoT device, we believe this range to be sufficient. The communication range that is achievable in a given deployment depends on the proximity and the output power of the carrier-generating node. In our case the carrier strength is limited to 0 dBm by the radio transceivers, much lower than carrier strengths used in other works [12, 15]. Nevertheless we believe that our experimental parameters are reasonably close to actual deployments.

This last assumption is supported by results from an IoT testbed with 100 nodes, where we observe carrier strengths in excess of -60 dBm in most locations. Such a carrier strength, in combination with a return loss up to 10 dB, is sufficient to ensure reception by nearby querying nodes.

In summary, our experimental results support the feasibility of our vision. Our proposal has the potential to ease the process of adding sensing capabilities to an existing network. It can also simplify the deployment process by separating sensing concerns from communication and power concerns.

Acknowledgments

This work has been funded by the Swedish Energy Agency and by the Internet Foundation in Sweden through Internetfonden.

7. REFERENCES

[1] ADF7242. http://www.analog.com/en/products/rf-microwave/integrated-transceivers-transmitters-receivers/low-power-rf-transceivers/adf7242.html.

[2] ATSAMR21g18a. http://www.atmel.com/devices/ATSAMR21G18A.aspx.

[3] CC2420. http://www.ti.com/product/CC2420.

[4] EFR32mg1b132f256gm32. https://www.silabs.com/products/wireless/mesh-networking/efr32-mighty-gecko/Pages/EFR32MG1B132F256GM32.aspx.

[5] MC13224v. http://www.nxp.com/products/microcontrollers-and-processors/arm-processors/kinetis-cortex-m-mcus/k-series-performance-m4/k3x-segment-lcd/2.4-ghz-802.15.4-rf-and-32-bit-arm7-mcu-with-128kb-flash-96kb-ram:MC13224V.

[6] Terasic - DE Main Boards - Cyclone - DE0-Nano Development and Education Board.

[7] Tmote sky datasheet. http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf.

[8] IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2011*, pages 1–314, 2011.

[9] C. A. Balanis. *Antenna Theory: Analysis and Design, 3rd Edition*. Wiley-Interscience, 3 edition edition, 2005.

[10] D. Bharadia, K. Joshi, M. Kotaru, and S. Katti. Backfi: High throughput wifi backscatter. SIGCOMM '15, pages 283–296. ACM, 2015.

[11] M. Doddavenkatappa, M. Chan, and A. Ananda. *Indriya: A Low-Cost, 3D Wireless Sensor Network Testbed*, chapter Testbeds and Research Infrastructure. Development of Networks and Communities: 7th International ICST Conference,TridentCom 2011, Shanghai, China, April 17-19, 2011, Revised Selected Papers, pages 302–316. Springer Berlin Heidelberg, 2012.

[12] J. F. Ensworth and M. S. Reynolds. Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices. In *2015 IEEE International Conference on RFID (RFID)*, pages 78–85, Apr. 2015.

[13] F. Ferrari, M. Zimmerling, L. Thiele, and O. Saukh. Efficient network flooding and time synchronization with Glossy. In *IPSN'11*, pages 73–84, 2011.

[14] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall. Wi-fi Backscatter: Internet Connectivity for RF-powered Devices. In *SIGCOMM'14*, pages 607–618. ACM, 2014.

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

[16] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith. Ambient Backscatter: Wireless Communication out of Thin Air. In *SIGCOMM'13*, pages 39–50. ACM, 2013.

[17] S. Naderiparizi, A. Parks, Z. Kapetanovic, B. Ransford, and J. R. Smith. Wispcam: A battery-free rfid camera. In *2015 IEEE International Conference on RFID*, pages 166–173, 2015.

[18] V. Talla and J. R. Smith. Hybrid analog-digital backscatter: A new approach for battery-free sensing. In *2013 IEEE International Conference on RFID*, pages 74–81, 2013.

[19] WISP 5.0. https://github.com/wisp/wisp5.

[20] H. Zhang, J. Gummeson, B. Ransford, and K. Fu. Moo: A batteryless computational rfid and sensing platform. Technical Report UM-CS-2011-020, University of Massachusetts Computer Science, 2011.

[21] P. Zhang, P. Hu, V. Pasikanti, and D. Ganesan. Ekhonet: High speed ultra low-power backscatter for next generation sensors. In *MobiCom '14*, pages 557–568. ACM, 2014.