

# How Manufacturers Can Easily Improve Working Range of Passive RFIDs

Ju Wang<sup>1</sup>, Liqiong Chang<sup>1</sup>, Omid Abari<sup>2</sup>, Srinivasan Keshav<sup>3</sup>

<sup>1</sup>Northwest University, <sup>2</sup>University of Waterloo, <sup>3</sup>University of Cambridge

{wangju,clq}@nwu.edu.cn, oabari@uwaterloo.ca, sk818@cam.ac.uk

**Abstract**—Radio-Frequency Identification (RFID) technology permits a reader to wirelessly query a tag for its embedded globally unique identifier. Passive RFID tags, which are small, low-cost (a few cents each), and batteryless, can be reliably read only when they are within a few meters of the reader since the tag must power up itself by harvesting energy from the reader. Past work attempts to increase the RFID range by providing them with more energy, such as by synchronizing multiple custom design RFID readers and performing beamforming. However, we demonstrate that a passive tag's range is limited not only by the need for the tag to harvest energy but also by the need for the tag to decode the reader's transmission, and *vice versa*. Thus, instead of modifying readers, we ask if a tag's manufacturer can increase passive RFIDs' range by lowering the data rate. Our results show that the working range can be increased by a factor of about 10 by simply using a low data rate. Our real-world experiments using customized tag prototypes have a range of ~40 m, with an SNR exceeding 12 dB.

**Index Terms**—RFID, Long Range, Bit Rate, Decoding Ability

## I. INTRODUCTION

Radio-Frequency IDentification (RFID) technology allows a reader to wireless query a tag for its unique digital ID. RFID tags can be either passive or active. Active RFID tags need a battery to transmit data, which not only adds to their cost, but also limits their lifetime. In contrast, passive RFID tags are batteryless, smaller, and cheaper. Thus, passive tags are widely used for applications in many industries [1], including agriculture, retail, security, and food.

Applications relying on passive RFID tags are critically limited by their range, that is, the distance at which they can be reliably read. This range is theoretically up to 10 m for Ultra High Frequency (UHF) based tags [2]. However, in practice, the robust working range of most RFID-based application systems is limited to 3-5 m, limiting their applicability [3]–[9]. Increasing the range of passive RFIDs would allow the development of many novel applications, such as the hands-free commercial and residential vehicle access [10] and the low-cost sensing [11]. Moreover, by sharing the cost of an expensive reader across a larger number of tags, they would reduce the overall deployment cost. Thus, this paper asks the question: *Can we increase the range of a passive RFID tag?*

Given the importance of passive RFID range, many prior researchers have addressed these question. However, prior

Liqiong Chang is the corresponding author. Part of this work was done at University of Waterloo. Ju Wang and Liqiong Chang on this work was partially supported by the National Natural Science Foundation of China under grant NO. 62172332 and 61802308.

studies have mostly focused on increasing the range by improving energy harvesting at passive RFID tags [12]–[17]. For example, some researchers propose to combine multiple customized RFID readers to perform beamforming [16]. However, these systems have two limitations. First, their performance gain is limited because harvesting energy is not the only reason for limiting a passive tag's working range: the need for the tag to decode the reader's transmissions and *vice versa* is also important. Thus, merely providing more energy to the tag is inadequate. Second, they require multiple readers and antennas which make the whole system both bulky (several meters across in size) and costly.

In this paper, we use a novel approach to solve the problem. Instead of treating the tag's parameters as a given, we show how to make a small modification to a tag (a modification that must necessarily be made by tag manufacturers), that can dramatically increase its range. Specifically, we first experimentally demonstrate that a tag's decoding ability is an important barrier to its working range. Then, we show how a manufacturer can improve a tag's decoding ability (and thus its range) by using a lower data transmission rate. This is because a low data rate improves the signal-to-noise ratio (SNR) of the communication paths of both the reader-to-tag and the tag-to-reader. We note that this approach has been well-studied in other contexts, such as the 802.11 technology [18], where there is an explicit choice of data rates to deal with environmental noise. However, to our knowledge, such a trade-off has never been proposed for RFID systems. Moreover, in our work, we experimentally measure the actual increase in range by reducing the data rate, something that is not obvious from theory alone.

We validate our insights using detailed real-world experiments. We first build a customized tag that mimics the operation of a low-bit-rate passive RFID tag. We then demonstrate that even existing tags can slightly improve their range by increasing the so-called 'Tari' value [19], which is the length of a symbol on the medium. Our experimental results show that with a low data rate, assuming enough energy can be harvested by a tag, the working range of a customized tag is as much as ~40 m, while keeping the SNR above ~12 dB. We conclude that by lowing the data rate of commodity RFID devices, something that a tag manufacturer can easily control, the maximum working range of passive RFID tags can be greatly improved.

This paper makes the following contributions:

- 1) We show that the energy harvesting problem is not the only limitation to the passive tag's working range.
- 2) We show how greatly increase the working range of passive RFID tags by using a low data rate.
- 3) We verify our solution through real-world experiments.

## II. BACKGROUND

Passive RFID tags are battery-free devices with unique embedded IDs that can be read by a device called an RFID reader. The reader transmits a high power Radio-Frequency (RF) signal as a query. The tag uses this query to power up itself and respond to the reader with its ID. To communicate a tag's ID to the reader, three conditions must be satisfied. First the tag needs to harvest enough energy from the reader's query signal. Second, the tag must decode the reader's query (this is the *downlink*). Third, the reader needs to successfully decode the tag's response (this is the *uplink*). We now explain each step in more details [19]:

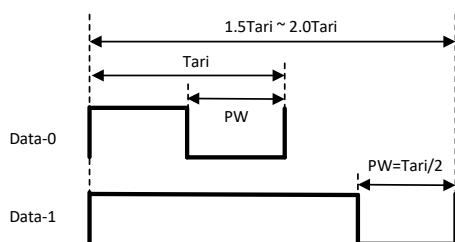


Fig. 1: Pulse Interval Encoding for RFID communication.

**Energy Harvesting.** To power up a passive RFID tag, the reader transmits a high power sinusoidal Continuous Wave (CW) signal which is used by the tag to harvest energy. Specifically, the tag uses a rectifying charge pump circuit to convert the CW signal into a Direct Current (DC) signal to power up its chip [20].

**Downlink.** Once the tag is powered up, it needs to decode the reader's query. RFID readers use Pulse Interval Encoding (PIE) scheme to communicate with tags [21]. In this scheme, the reader transmits its query bits by emitting pulses of CW signal with varying intervals, as shown in Fig. 1. To transmit a '0' bit, the reader transmits the CW signal for a short time followed by a short period of silence; to transmit a '1' bit, the reader does the same, except that the CW signal lasts for a longer time. The length of a bit is defined by the 'Tari' value which can be chosen from  $6.25 \mu\text{s}$  to  $25 \mu\text{s}$  in today's RFID tags. The tag decodes the reader's query signal by monitoring the power level of the query signal using a rectifier circuit (see Section IV for details).

**Uplink.** Once the tag decodes the reader's query, it responds to the reader with its embedded ID. The tag uses ON-OFF Keying (OOK) modulation to communicate with the reader. Specifically, the tag transmits a '1' bit by reflecting the reader's signal and a '0' bit by not reflecting the signal. On the reader side, the reader uses full-duplex hardware to remove its self-interference signal (i.e., the reader's high power CW signal),

and then uses an RF chain and an Analog-to-Digital Converter (ADC) to down-convert and decode the tag's ID.

## III. MOTIVATION AND OUR SCOPE

For an RFID reader to successfully read a tag, three conditions must be met: the tag should be able to harvest enough energy, the tag should be able to decode the reader's query signal, and the reader should be able to decode the tag's response signal. Most prior researchers focus on only the first step [12]–[17]. Thus, they attempt to improve a tag's working range by delivering more power to the tag. Although, these approaches are effective to some extent, the tag's range and reliability continue to be limited due to the second and third requirements, which arise *the motivation of this paper*.

### A. Motivation

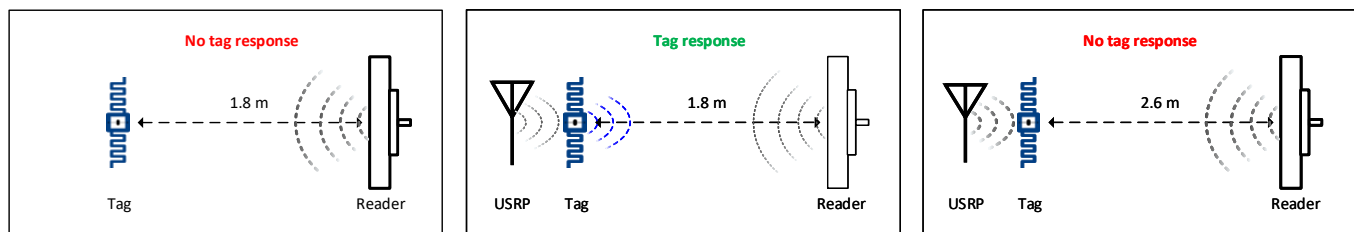
We demonstrate the aforementioned results and our motivation by using three real-world experiments. We use an ALN-9740 RFID tag [22], an Impinj R420 RFID reader [23], and an Ettus USRP N210 [24]. The USRP transmits a continuous sine wave at a frequency of 850 MHz. This sine wave signal is used to power up the tag, so that the tag is never energy-limited. Note that, although RFID readers and tags can work in a wide range of frequencies (840 MHz and 960 MHz), our reader operates only at the frequency range of 902.75–927.25 MHz [23], due to the Federal Communications Commission (FCC) regulation. This guarantees that the power signal (i.e., the sine wave at 850 MHz) generated by the USRP will not create interference for the reader, and the reader will be able to read the tag's ID.

*Experiment 1:* In this experiment, as shown in Figure 2(a), an RFID tag is deployed 1.8 m away from a reader that operating at a low transmission power (i.e., 10 dBm). At this transmission power, the tag does not respond to the reader.

*Experiment 2:* We perform the same experiment as 'Experiment 1', while we deploy a USRP 10 cm away from the tag, as shown in Figure 2(b). The USRP transmits a continuous sine wave to provide additional power to the tag. Then, the reader can read the tag. This implies that the range of the tag was limited by the amount of energy it could harvest.

*Experiment 3:* We perform the same experiment as 'Experiment 2' while we increase the tag-to-reader distance from 1.8 m to 3.0 m with a step of 10 cm, and check if the tag responds to the reader, as shown in Figure 2(c). Note that, similar to 'Experiment 2', we always keep the USRP 10 cm away from the tag, so that the tag is not energy-limited. We find that when the distance between the tag and the reader increases beyond 2.6 m, the reader cannot read the tag. This continues to be true even when we increase the transmission power of the USRP to provide more power to the tag.

*Conclusion:* The above experiments imply that even if a tag can harvest enough energy to power up itself, its range can still be limited due to its inability to decode the reader's query signal or the reader's inability to decode the tag's response signal. Because, as the distance between the tag and the reader increases, the SNR of both reader's query signal and the tag's



(a) Exp-1. The tag does not respond due to the reader's low transmission power. (b) Exp-2. Additional power is added to the tag. Now, the tag can respond to the reader. (c) Exp-3. Even with enough energy, the range is limited by the decoding capability of tag and reader.

Fig. 2: Experiments for observing the working range limitations of RFIDs.

response signal decreases and hence one or both signals cannot be decoded, resulting in a limited range.

### B. Scope of Our Work

Recent work has demonstrated several techniques to provide more power to RFID tags, so that the tags are never energy-limited [12]–[17]. Thus, we assume in our work that the energy harvesting problem has been solved using one of these approaches, and focus only on how to improve the decoding ability of RFID readers and tags.

## IV. IMPROVING DECODABILITY

We now explain our approach to improving the tag's ability to decode the reader's query (downlink) and the reader's ability to decode the tag's response (uplink) in a low SNR regime.

### A. Improving Downlink Decoding

We first explain how RFID tags decode a reader's signal, then provide insights of improving the downlink decoding.

A simplified demodulator of typical passive RFID tags is shown in Figure 3. The demodulator works as an envelope detector, which includes a diode, a capacitor, and a resistor. When there is an RF signal at its input, the capacitor is charged and the output voltage of the demodulator goes high (i.e., the high-level voltage); and when there is no signal at the input, the capacitor is discharged by the resistor and the output voltage drops (i.e., the low-level voltage). An RFID tag decodes the reader's query message by distinguishing the voltages between these two levels, e.g., a low-level voltage means '0' bit and a high-level voltage means a '1' bit. For example, Figure 4 (top) shows an reader's query signal<sup>1</sup> which goes into the input of the demodulator, and the below figure shows the signal at the output of the demodulator. Clearly, the '1' bit and '0' bit can be detected by distinguishing the two voltage levels.

The downlink decodability diminishes when the distance between the reader and the tag increases, so that the difference between these two voltage-levels decreases, which makes it hard for the tag to distinguish between the '1' bit and the '0' bit. To improve a tag's range, that is, its ability to decode the reader's query, we need to increase the voltage gap  $V$  between the high-level and the low-level voltages, as shown in Figure 4.

<sup>1</sup>As described in Section II, the reader transmits its query's bits by emitting pulses of the CW signal.

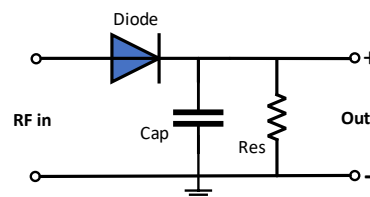


Fig. 3: A simplified demodulator of RFID tags.

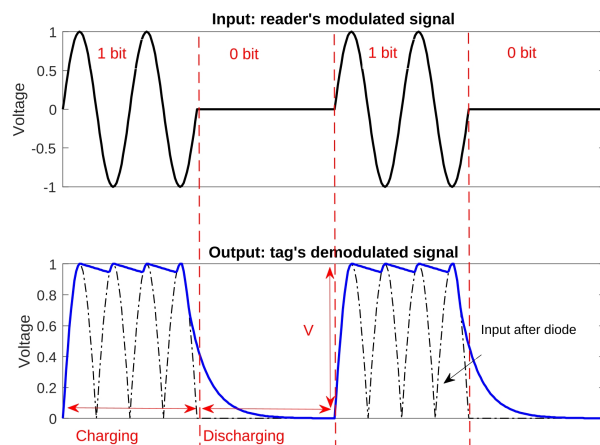


Fig. 4: An example of a reader's modulated signal and a tag's demodulated signal.

That is to say, *the larger the voltage gap is, the easier for a tag to differentiate between the two voltage-levels, resulting in an improved downlink decoding.*

Note that the high-level voltage is equal to the amplitude of the input signal and the low-level voltage is the voltage of the capacitor when it is discharged. For a given tag-to-reader's distance, the amplitude of the input signal is fixed. Thus, in order to increase the voltage gap  $V$ , we need to make sure that the capacitor has enough time to be fully discharged, thus lowering the low-level voltage.

To understand the relationship between the discharge time and the capacitor voltage, assume that  $U_i$  is the voltage amplitude of the input RF signal. Then, Equation (1) shows the output voltage  $U_o$ , i.e. the voltage of the capacitor, when the capacitor is discharging over time  $t$  as:

$$U_o = U_i \cdot e^{-\frac{t}{RC}}, \quad (1)$$

where  $R$  and  $C$  are the resistance and the capacitance of a tag's demodulator. Clearly, the output voltage  $U_o$  decays exponentially over time, i.e., the longer the discharge time, the lower the ultimate output voltage. Therefore, to increase the voltage gap  $V$ , either we need to increase the capacitor's discharge time or decrease the value of  $RC$ .

Tuning the  $RC$  value of the tag's envelope detector is a plausible alternative to improving a tag's ability to decode the reader's query. However, we use simulations to demonstrate that in fact, this is not a practical approach. We set up a simulation using the Matlab Simulink package [25] to model the behaviour of the envelope detector, i.e., a simple  $RC$  circuit. Figure 5 shows the impact of the  $RC$  value on the envelope detector's output signal for three different  $RC$  values. We make the following observations:

- *Large  $RC$  value:* When the  $RC$  value is too large, the capacitor will discharge slowly, as shown in Figure 5(a). Thus, the voltage gap  $V$  will be very small, reducing a tag's decoding ability.
- *Small  $RC$  value:* When the  $RC$  value is too small, the capacitor discharges very fast, as shown in Figure 5(b). In this case, the capacitor voltage simply follows the rectified sine wave and hence the circuit does not work as an envelope detector, i.e. the tag does not decode.
- *Carefully-chosen  $RC$  value:* When we carefully choose values for  $RC$ , as shown in Figure 5(c), the demodulator works as an envelope detector and the capacitor discharges when there is no input signal. We may get a large voltage gap  $V$  when the capacitor is fully discharged.

*Conclusion:* Those results imply that the choice of the  $RC$  value is tightly constrained and cannot be easily tuned to increase a tag's decoding ability.

To this end, it leaves the only feasible alternative: reducing the low-level voltage by increasing the discharging time, i.e., using a low data rate. Specifically, by increasing the '*Tari*' illustrated in Figure 1, the RFID tag's capacitor will have more time to discharge and hence the low-level voltage will be more distinguishable from the high-level voltage. By doing so, we can improve the ability of the tag to decode a reader's query and also increase the tag's communication range. We experimentally validate this insight in Section V.

### B. Improving Uplink Decoding

In this section, we first explain how a reader decodes a tag's response; then discuss how using a low data rate improves the reader's ability to decode this response.

As explained in Section II, the tag uses the ON-OFF keying modulation to communicate with the reader. The tag transmits a '1' bit by reflecting the reader's signal and '0' bit by not reflecting it. The reader uses (i) a full-duplex hardware to remove its self-interference signal, (ii) a standard RF chain to down-convert the RF signal to the baseband, and (iii) an ADC to sample and decode the tag's response signal. The reader's decoding ability is limited by the SNR of the sampled signal: if this SNR is too low, the reader will be unable to decode the tag's response. Hence, in order to improve the reader's

decoding ability when the tag is distant from the reader, we need to improve the SNR of the tag's response signal.

To understand how to do so, we first recall that SNR is defined as the ratio of the signal power to the noise power, and can be calculated as:

$$SNR(dB) = 10 \log_{10} \frac{\text{Signal Power}}{\text{Noise Power}}. \quad (2)$$

Crucially, noise values are uncorrelated and signal values are linearly correlated. Hence, if we sum a large number of received signal samples (i.e., noisy signals), the averaged noise power will decline by the number of averaged samples, while the averaged signal power will be nearly constant. Mathematically, the SNR (i.e.,  $SNR_{avg}$ ) after the averaging process over  $W$  samples is:

$$SNR_{avg} = 10 \log \left( \frac{\text{Averaged Signal Power}}{\text{Averaged Noise Power}} \right) \quad (3)$$

$$\approx 10 \log \left( \frac{\text{Initial Signal Power}}{\text{Initial Noise Power}/W} \right) \quad (4)$$

$$= SNR_{initial} + 10 \log(W), \quad (5)$$

where,  $SNR_{initial}$  is the SNR before the averaging process. This equation shows that averaging  $W$  samples will improve the SNR by  $10 \log(W)$  dB. Note that the averaging can be done in the reader's software and does not require modifications of the reader's hardware.

To this end, to improve the SNR, we simply need to average samples for a relatively long period of time: this keeps the signal power constant, while the noise power declines. To evaluate this in practice, we experimentally compute the power of averaged signals and the power of averaged noise from USRP samples. Figure 6 shows the result, where we increase the number of samples  $W$  to be averaged from 1 to 200. As expected, with the increase of the number of samples  $W$ , the power of averaged signals stays constant, whereas the power of averaged noise decreases. Note that, when the number of samples  $W$  is larger than 100, the power of averaged noise decreases slowly, since it reaches the non-white noise floor.<sup>2</sup> Indeed, the averaging only helps in reducing the white noise, it does not reduce some other sources of noise (such as the ADC non-linearity noise) which are not white.

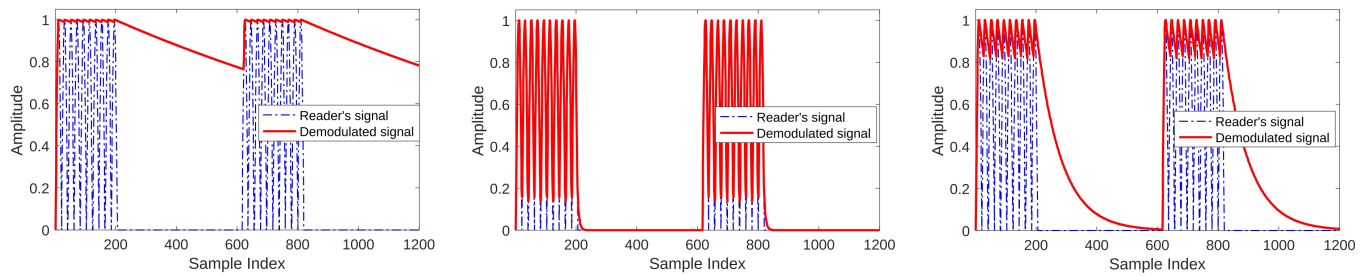
## V. RESULTS

In this section, we conduct experiments to verify our ideas. We first verify if lowering the data rate improves the tag's ability to decode the reader's query. Next, we verify if lowering the data rate improves the reader's ability to decode the tag's response. Finally, we verify if lowering the data rate improves the range of commodity passive RFID tags.

### A. Downlink

We begin by examining whether using a low data rate can improve a tag's ability to decode a reader's query in the low SNR regime.

<sup>2</sup>Note that one can further improve the SNR by using a better hardware and a larger window size beyond 100. In our experiment, the non-white noise floor of the USRP is high due to the poor quality of hardware.



(a) A large  $RC$  value. The capacitor discharges slowly and the voltage gap is small, reducing a tag's decode ability.

(b) A small  $RC$  value. The capacitor discharges very fast and the demodulator does not work, i.e. the tag does not decode.

(c) A carefully-chosen  $RC$  value. The demodulator works as a detector and we may get a large voltage gap when the capacitor is fully discharged.

Fig. 5: Impact of  $RC$  values on the voltage gap between a tag's demodulated signal and a reader's signal after the diode.

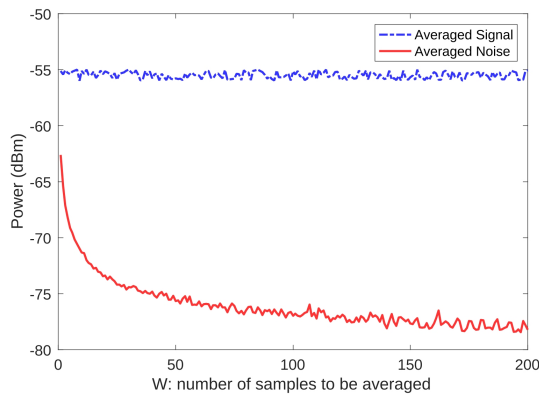
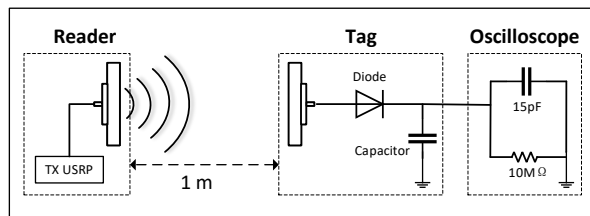
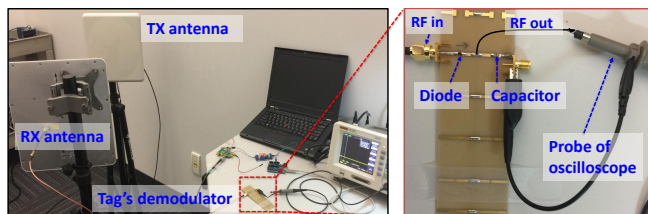


Fig. 6: An example of improving SNR by averaging the received signal samples.



(a) The deployment layout.



(b) The experimental scene.

Fig. 7: The experimental deployment layout in (a) and the scene in (b) for verifying the downlink SNR improvement.

1) *Implementation*: We use an Ettus USRP N210 [24] with a typical RFID antenna to act as an RFID reader, as shown in Figure 7(a). The directional antenna has a gain of 9 dBi and a beam width of  $63^\circ$  [26]. The USRP transmits a PIE modulated sine wave signal with a frequency of 915 MHz and a gain of 30 dB. We also build an RFID tag's demodulator

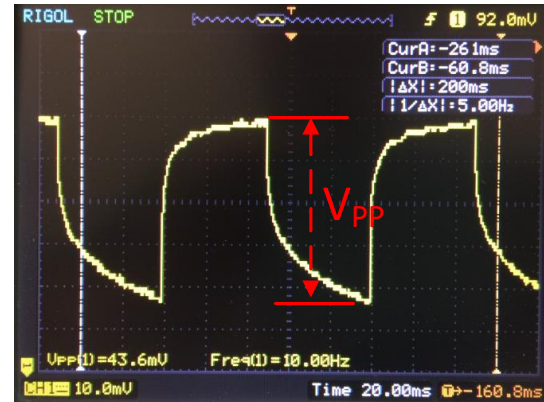


Fig. 8: An illustration of a tag's demodulated signal.

that similar to the one used in commodity RFID tags. The demodulator includes an antenna, a capacitor, and a diode with a low forward voltage of 0.38 V [27]. The diode and the capacitor work as a passive envelope detector to demodulate reader's signals. This custom-designed tag and reader allow us to run experiments at different data rates and also measure the voltage of the tag's demodulated signal.

The modulated signal transmitted by the USRP (i.e., the reader) is received by the tag. Then, the tag demodulates the received reader's signal into a square signal, which has high-level and low-level voltages that indicate '1' bit and '0' bit. We expect to have a large voltage gap, since it improves the tag's decoding ability and working range as explained in Section IV. To measure the voltage gap, we connect the output of the tag's demodulator to an oscilloscope.

2) *Evaluation*: We conduct our experiments in an office space as shown in Figure 7(b). We perform experiments for different data rates and different capacitance values of the tag's demodulator. Specifically, the data rates (i.e., the PIE modulation frequencies) are 10 Hz, 100 Hz, 1 KHz, 10 KHz, 65 KHz and 128 KHz; and the capacitance values are 15 pF, 470 pF, 1 nF, 470 nF and 1 uF. For each data rate and capacitance, we use the oscilloscope to measure  $V_{pp}$  of the output signal of the demodulator.

Figure 8 shows a screen shot of the oscilloscope measured output signal of the tag's demodulator, when the capacitor value is 15 pF and the data rate (or frequency) is 10 Hz. The

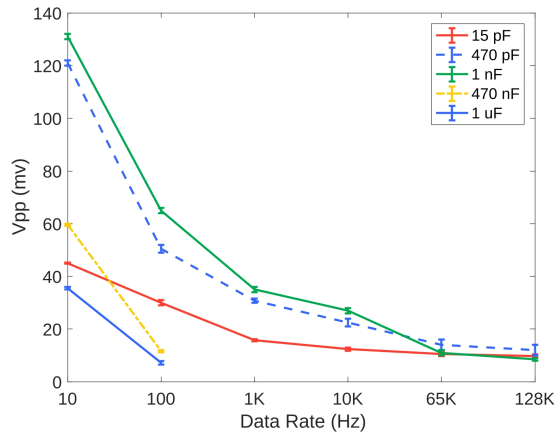


Fig. 9: The voltage gap  $V_{pp}$  versus different data rates.

oscilloscope automatically measures the Peak-to-Peak Voltage ( $V_{pp}$ ) between the high and low levels of the demodulated signal. The figure clearly shows that our circuit works as a demodulator, since the two level voltages are very different.

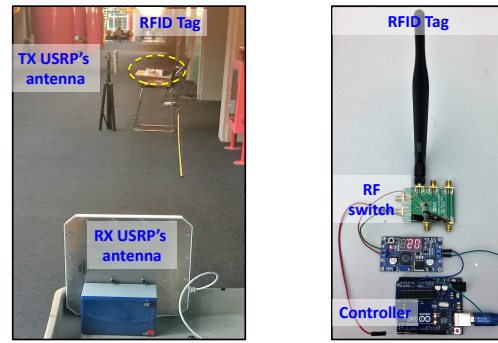
Figure 9 shows  $V_{pp}$  for different data rates and capacitance values. As we can see,  $V_{pp}$  decreases when we increase the data rate. It implies that, as expected, using a lower data rate results in a longer operating range for RFID tags. We also see, confirming our theoretical analysis, that  $V_{pp}$  is sensitive to the capacitance values. Indeed, when the capacitor is oversized (e.g.,  $> 1 \mu\text{F}$ ), the circuit ceases to act as a demodulator.

### B. Uplink

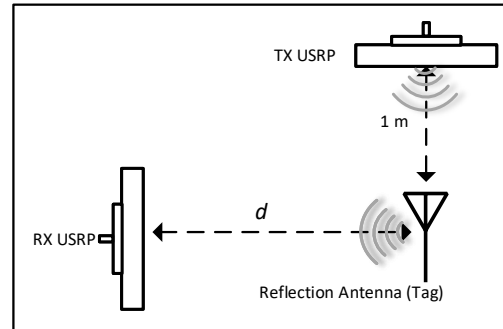
We now examine whether using a low data rate improves the reader's ability to decode a tag's response signal in the low SNR regime.

1) *Implementation:* We use two USRPs with two directional antennas to implement the transmitting chain and the receiving chain of an RFID reader, as shown in Figure 10. The 'TX USRP' transmits a continuous sine wave signal with a gain of 30 dB and a frequency of 915 MHz. We design an omni-directional RF reflector to act as the RFID tag, as shown in Figure 10(a). The RF reflector consists of an omni-directional VERT900 antenna [28], an analog device ADG902 RF switch [29] and an Arduino UNO controller [30]. The ADG902 RF switch connects the antenna's port to the ground or keep the antenna's circuit open. When the antenna is open-circuit, it does not reflect an incoming signal; when the antenna is connected to the ground, the antenna reflects the incoming signal. An Arduino controls the OOK modulation frequency (i.e. the data rate) of the ADG902 RF switch. The 'RX USRP' receives the reflection signal from the tag.

2) *Evaluation:* To minimize the interference between the 'TX USRP' and the 'RX USRP', the tag-to-TX's link and the tag-to-RX's link are deployed perpendicular to each other, as shown in Figure 10(b). The distance between the tag and the 'TX USRP' is 1 m. The distance  $d$  between the tag and the 'RX USRP' is set to  $d=1$  m, 6 m, 18 m, 30 m, 36 m, and



(a) The experimental scene.



(b) The deployment layout.

Fig. 10: The experimental scene in (a) and the deployment layout in (b) for verifying the uplink SNR improvement.

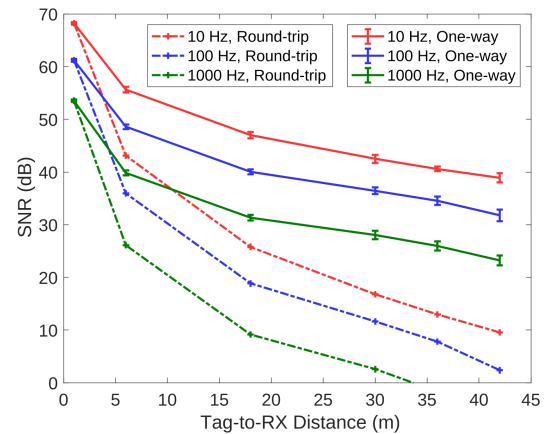


Fig. 11: SNR versus the distance for different data rates.

42 m. For each distance  $d$ , we test three different data rates: 10 Hz, 100 Hz and 1000 Hz.

We measure the SNR of the averaged signal, as described in Section IV-B, for different data rates and different distances  $d$ . Figure 11 shows the results of this experiment. Since we fix the distance between the 'TX USRP' and the tag as 1 m, our results calculate the one-way (i.e., the tag to 'RX USRP' link) SNR measurements, as the three solid lines shown in Figure 11. To estimate the expected SNR of a round-trip signal, we first use the one-way SNR measurement when  $d=1$  m as the baseline, since the distance of the tag-to-'TX USRP' is 1 m. Then, we calculate the one-way SNR

differences between the baseline and the SNR at a distance  $d$ . Next, for each distance  $d$ , we subtract double of the SNR difference from the baseline SNR to get the round-trip SNR measurements. For example, suppose that the one-way SNR at 1 m and  $d$  are  $x_{base}$  and  $x_d$ . Then, the two-way SNR at  $d$  is  $x'_d = x_{base} - 2(x_{base} - x_d)$ .

As expected, increasing the distance between the tag and the reader degrades the SNR. However, we find that for a fixed distance, reducing the data rate significantly improves the SNR of the averaged signal, which results in a higher working range for RFID tags. It is clear that there is a trade-off between the data rate (i.e., the OOK modulation frequency) and the maximum working range. Specifically, to achieve a specific SNR, a lower data rate gives us a longer working range. For example, a range of more than 40 m with an SNR of 12 dB is achievable when the data rate is 10 Hz, as the red dashed line shown in Figure 11. Note that, the OOK modulation can achieve a bit error rate of  $10^{-4}$  at the SNR of 12 dB [31], which provides an efficient communication for RFID tags.

Further, it is worth mentioning that these results are based on the 30 dBm transmission power, which is in accordance with the FCC rules and the commodity RFID reader's transmission power.

### C. Improving the Range of Commodity Passive RFID Tags

So far, we have showed how to use the low data rate to improve the decoding ability of both a tag and a reader. Here, we examine whether we can use this insight to increase the working range of commodity RFID tags.

1) *Implementation:* We use an Impinj R420 RFID reader [23] without any modification. The reader operates in a frequency range of 902.75–927.25 MHz. The antenna used by the reader is a directional antenna with a 9 dBi gain and 63° elevation and azimuth beam widths [26]. We test three RFID tags with three kinds of chips:

- 1) 'Tag 1': Alien Squiggle ALN-9740 RFID tag with the Alien Higgs-4 chip [22].
- 2) 'Tag 2': SMARTRAC Frog 3D RFID tag with the Impinj Monza 4D chip [32].
- 3) 'Tag 3': INLAY DRY AD-383U7 tag with the NXP UCODE 7 chip [33].

The reader and tags used in our experiments are the same as the readers used in state-of-the-art RFID systems [34]–[37].

2) *Evaluation:* As explained in Section II, a reader communicates with a tag using the Pulse Interval Encoding (PIE) modulation scheme. Therefore, in order to change the data rate, we change the pulse period which can be done by changing the 'Tari' value.<sup>3</sup>

Ideally, we would like to change the data rate from a few Hz to a few MHz and see how it impacts on the operating range of RFIDs. This means that we need to change the 'Tari' value from a few  $\mu s$  to hundreds of  $ms$ . However, existing RFID tags and readers only allow changing the 'Tari' value

<sup>3</sup>Recall that the 'Tari' value determines the length of the '0' bit and the '1' bit for the reader-to-tag's communication, as explained in Section II.

TABLE I: RFID Reader Settings

LLRP Mode/ Name	Tari (us)	PIE
0 / Max Throughput	6.25	1.5:1
1 / Hybrid Mode	6.25	1.5:1
2 / Dense Reader (M=4)	20	2:1
3 / Dense Reader (M=8)	20	2:1
4 / Max Miller	7.14	1.5:1

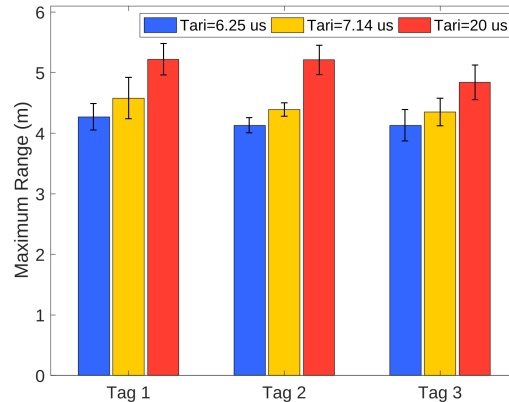


Fig. 12: The maximum working range of RFIDs under different 'Tari' values, where reader's power is 20 dBm.

over a small range (i.e., 6.25  $\mu s$  to 20  $\mu s$ ). Table. I shows the reader's working modes. We test three modes with three different 'Tari' values, i.e., (i) 'Mode 1' with Tari = 6.25  $\mu s$ ; (ii) 'Mode 4' with Tari=7.14  $\mu s$ ; (iii) 'Mode 2' with Tari=20  $\mu s$ . For each 'Tari' value, we measure the maximum working ranges of all the three tags when we set the transmission power of the reader as 20 dBm. The results are shown in Figure 12. As we can see, increasing the 'Tari' value increases the RFIDs' working range since a larger 'Tari' value means a lower data rate, which verifies our insight.

We also observe that increasing the 'Tari' value by  $\sim 3$  times improves the range by  $\sim 30\%$ . Although, the 30% improvement in the working range might not seem significant, if the software of the reader and the tag allows to change 'Tari' value from a few  $\mu s$  to tens of  $ms$ , the working range can significantly be improved (by up to 10 times).

## VI. RELATED WORK

We discuss the related work in both the RFID studies and the recent long-range backscatter networks.

### A. Improving the RFID Range by Using Multiple Readers

One solution to extend the RFID range is to use multiple antennas [38], [39] or multiple readers [17]. For example, an Impinj R420 reader can support 4 antennas [23]. One can place these antennas in different locations to cover a larger area or a longer distance. However, this approach adds additional cabling complexity and requires expensive and bulky readers which can support multiple antennas. Moreover, this approach still has limited range since each reader can only support

a small number of antennas. Recent work [17] uses the collaboration between multiple readers to enhance the range of some passive RFID tags. However, this approach can not active/read all tags deployed in an area. Another work [16] proposes synchronizing multiple antennas to perform beam-forming to increase RFID's working range. However, this solution requires expensive clock, 8 USRPs and 8 antennas. Further, since reader's antennas are bulky and they need to be placed half-wavelength apart from each other, this solution requires a large spatial footprint which may not be feasible in many scenarios.

Another solution to improve the RFID range is to deploy a repeater on a drone [40] or multiple edge devices in the environment to cooperate with the RFID reader for reading RFID tags [41]. However, the design and deployment of many edge devices is not cost-effective at the present time. Also, placing a repeater on a drone [40] is not feasible in many environments such as homes or hospitals.

Unlike these solutions, the method introduced in this paper can improve the working range of RFID systems without the need of additional hardware or antennas. Our method only needs a data rate modification in the reader's software and a support of low data rates at the tags.

#### B. Improving the RFID Range by Harvesting More Energy

Past work has also attempted to solve the range limitation problem by allowing tags to harvest more energy. These ideas can be classified into two categories.

The first category introduces an additional power source into the RFID tag. Those systems use either solar cells [12], batteries [13] or oscillators [14] as an additional source of power. Thus, they can improve the working range of RFIDs by providing more energy to the tag. The system proposed in Reference [14] uses a solar cell to collect DC power, and then the collected DC power is converted to the RF power using a high efficiency oscillator. Finally, the RF power is fed into the RFID tag to improve its working range. Similarly, Vijay *et al* [13] design a small battery powered RFID integrated circuit (IC) for operation at the ultra high frequency and microwave bands, in order to improve the working range of RFID tags. However, these solutions require extensive hardware modification.

The second category of solutions works on the reader side and tries to optimize the reader's transmission signal so that the tag can harvest more energy [15], [42]. For example, in Reference [15], the RFID reader transmits a Power Optimized Waveform (POW), rather than a traditional continuous wave (CW). The average transmission power of POW and CW are the same, but the POW produces a short time window of large voltage peaks. As a result, the RFID tag can harvest more energy. Thus, compared with the traditional CW, the tag's range is improved, given the same transmission power.

In contrast to those studies, this paper demonstrates that a passive RFID tag's range is limited not only by the need of the tag to harvest energy but also by the need of the tag to decode a reader's signal, and *vice versa*. We propose a simple solution

to improve the ability of a tag and a reader to decode each other's signals, and hence significantly improve the working range of RFID systems.

#### C. Improving the Range by Designing New Readers and Tags

Some studies try to improve the RFID range by designing new readers [42] or new tags [43], [44]. For example, Boaventura *et al.* [42] design a multi-sine front-end reader that can generate high peak power signals for improving the RFID range. Such as, Amato *et al.* [43] and Varshney *et al.* [44] design tunnel diode-based RFID tags that exhibit higher RF power gain and lower power consumption, thus achieving a long RFID range.

Unfortunately, it is costly to redesign tags or readers due to the production line rebuilding, additional testing and the challenge of Compatibility with existing RFID devices, making those solutions infeasible for manufacturers. In contrast, our solution only needs software changes, which allows manufacturers to improve the RFID range easily at a low-cost.

#### D. Long-Range Backscatter Networks

Recently, the long-range backscatter networking has garnered significant attention [45]–[47]. A state-of-the-art system such as HitchHike [45] works with existing Wi-Fi devices and achieves a reading range of 34 m when the transmitter is 1 m away from the tag. LoRa backscatter can achieve a longer range but it requires either a battery [46] or a super-capacitor [47] to provide energy to the tag. The range limitation of these systems is similar to RFIDs. Specifically, to power up their backscatter tags, the tags need to receive sufficient power from a transmitter. Thus, the energy problem is still the limitation for their long range. However, none of those systems discuss whether the decoding ability limits their working range. We hope this paper also provides some insight for improving the working range of such long-range, backscatter systems.

## VII. DISCUSSION AND CONCLUSION

We demonstrate that the working range of RFID systems is limited not only by the energy a tag harvested, but also the ability of the tag to decode a reader's signal and *vice versa*. Therefore, to improve the working range and decoding ability of RFID systems, we propose a simple solution, which is to use a low data rate. It is worth mentioning that existing RFID chips do not allow changing data rates over a wide range, hence we are planing to build our own RFID chips in future. However, our real-world experiments, using our tag prototype, show that the working range of RFID tags can be improved by up to 10× using our solution. We believe that our solution opens up numerous exciting applications for RFID systems.

## REFERENCES

- [1] E. Ilie-Zudor, Z. Kemény, F. Van Blommestein, L. Monostori, and A. Van Der Meulen, "A survey of applications and requirements of unique identification systems and RFID techniques," *Elsevier Computers in Industry*, vol. 62, no. 3, pp. 227–252, 2011.



- [2] Impinj, "Impinj RFID reader low level data support." <https://support.impinj.com/hc/en-us/articles/202755318-Application-Note-Low-Level-User-Data-Support>, 2013. Last accessed: July 17, 2018.
- [3] J. Wang, F. Adib, R. Knepper, D. Katabi, and D. Rus, "Rf-compass: Robot object manipulation using RFIDs," in *Proc. ACM MobiCom*, pp. 3–14, 2013.
- [4] J. Wang, L. Chang, S. Aggarwal, O. Abari, and S. Keshav, "Soil moisture sensing with commodity rfid systems," in *Proc. ACM MobiSys*, pp. 273–285, 2020.
- [5] J. Wang, J. Li, M. H. Mazaheri, K. Katsuragawa, D. Vogel, and O. Abari, "Sensing finger input using an rfid transmission line," in *Proc. ACM SenSys*, pp. 531–543, 2020.
- [6] K. Katsuragawa, J. Wang, Z. Shan, N. Ouyang, O. Abari, and D. Vogel, "Tip-tap: battery-free discrete 2d fingertip input," in *Proc. ACM UIST*, pp. 1045–1057, 2019.
- [7] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile RFID tags to high precision using cots devices," in *Proc. ACM MobiCom*, pp. 237–248, 2014.
- [8] T. Wei and X. Zhang, "Gyro in the air: tracking 3d orientation of batteryless internet-of-things," in *Proc. ACM MobiCom*, pp. 55–68, 2016.
- [9] H. Ding, J. Han, A. X. Liu, J. Zhao, P. Yang, W. Xi, and Z. Jiang, "Human object estimation via backscattered radio frequency signal," in *Proc. IEEE INFOCOM*, pp. 1652–1660, 2015.
- [10] J.-D. Tseng, W.-D. Wang, and R.-J. Ko, "An UHF band RFID vehicle management system," in *IEEE International Workshop on Anti-counterfeiting, Security, Identification*, pp. 390–393, 2007.
- [11] J. Wang, O. Abari, and S. Keshav, "Challenge: RFID hacking for fun and profit," in *Proc. ACM MobiCom*, pp. 1–10, 2018.
- [12] J. Kimionis, A. Georgiadis, S. Kim, A. Collado, K. Niotaki, and M. M. Tentzeris, "An enhanced-range RFID tag using an ambient energy powered reflection amplifier," in *IEEE MTT-S International Microwave Symposium*, pp. 1–4, 2014.
- [13] V. Pillai, H. Heinrich, D. Dieska, P. V. Nikitin, R. Martinez, and K. S. Rao, "An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 na at 1.5 v," *IEEE Transactions on Circuits and Systems*, vol. 54, no. 7, pp. 1500–1512, 2007.
- [14] A. Georgiadis and A. Collado, "Improving range of passive RFID tags utilizing energy harvesting and high efficiency class-e oscillators," in *European Conference on Antennas and Propagation*, pp. 3455–3458, 2012.
- [15] M. S. Trotter, J. D. Griffin, and G. D. Durgin, "Power-optimized waveforms for improving the range and reliability of RFID systems," in *IEEE International Conference on RFID*, pp. 80–87, 2009.
- [16] Y. Ma, Z. Luo, C. Steiger, G. Traverso, and F. Adib, "Enabling deep-tissue networking for miniature medical devices," in *Proc. ACM Sigcomm*, pp. 417–431, 2018.
- [17] J. Wang, J. Zhang, R. Saha, H. Jin, and S. Kumar, "Pushing the range limits of commercial passive rfids," in *Proc. USENIX NSDI*, pp. 301–316, 2019.
- [18] D. Pong and T. Moors, "Fairness and capacity trade-off in ieee 802.11 wlans," in *IEEE international conference on local computer networks*, pp. 310–317, 2004.
- [19] E. EPCglobal, "Radio frequency identity protocols generation 2 UHF RFID," *Specification for RFID Air Interface, Protocol for Communications*, vol. 860, 2004.
- [20] A. Shamel, A. Safarian, A. Rofougaran, M. Rofougaran, and F. De Flaviis, "Power harvester design for passive UHF RFID tag using a voltage boosting technique," *IEEE Transactions on Microwave Theory and Techniques*, vol. 55, no. 6, pp. 1089–1097, 2007.
- [21] E. Inc, "Low level reader protocol, version 1.0. 1," 2007.
- [22] A. T. Corp., "UHF aln-9740 tag." <https://www.atlasrfidstore.com/alien-squiggle-rfid-white-wet-inlay-aln-9740-higgs-4/>, 2017. Last accessed: July 17, 2018.
- [23] Impinj, "Impinj r420 readers." <http://www.Impinj.com/products/readers/>, 2010. Last accessed: June 27, 2018.
- [24] N. Instruments, "Ettus usrp n210." <https://www.ettus.com/product/details/UN210-KIT>, 2018. Last accessed: July 17, 2018.
- [25] M. Inc., "Rc circuit in simulink and simscape." <https://www.mathworks.com/help/phymod/simscape/examples/rc-circuit-in-simulink-and-simscape.html>, 2018. Last accessed: July 27, 2018.
- [26] Atlasrfidstore, "Rfmax RFID race timing antenna." <https://www.atlasrfidstore.com/rfmax-rfid-race-timing-antenna-kit-15-ft-cable/>, 2018. Last accessed: July 27, 2018.
- [27] Onsemi, "Silicon hot-carrier diodes." <https://www.onsemi.com/pub/Collateral/MMDL301T1-D.PDF>, 2018. Last accessed: Nov. 27, 2018.
- [28] N. Instruments, "Vert900 vertical antenna." <https://www.ettus.com/product/details/VERT900>, 2018. Last accessed: Nov. 27, 2018.
- [29] A. D. Inc., "Adg902 rf switch." <https://www.digikey.ca/product-detail/en/analog-devices-inc/ADG902BRMZ/ADG902BRMZ-ND/997618>, 2018. Last accessed: Nov. 27, 2018.
- [30] Arduino, "Arduino uno." <https://www.digikey.ca/product-detail/en/arduino/A000073/1050-1041-ND/3476357>, 2018. Last accessed: Nov. 27, 2018.
- [31] Q. Tang, S. K. Gupta, and L. Schwiebert, "Ber performance analysis of an on-off keying based minimum energy coding for energy constrained wireless sensor applications," in *Proc. IEEE ICC*, vol. 4, pp. 2734–2738, 2005.
- [32] S. Corp., "UHF smartrac frog 3d tag." <https://www.atlasrfidstore.com/smartrac-frog-rfid-wet-inlay-monza-4d/>, 2013. Last accessed: July 17, 2018.
- [33] A. D. Corp., "UHF ad-383u7 tag." <http://rfid.averydennison.com/content/dam/averydennison/rfid/Global/Documents/datasheets/AD-383u7-Datasheet-v1.pdf>, 2017. Last accessed: July 17, 2018.
- [34] J. Wang, J. Xiong, X. Chen, H. Jiang, R. K. Balan, and D. Fang, "Tagscan: Simultaneous target imaging and material identification with commodity rfid devices," in *Proc. ACM MobiCom*, pp. 288–300, 2017.
- [35] J. Wang, J. Xiong, H. Jiang, X. Chen, and D. Fang, "D-watch: Embracing bad multipaths for device-free localization with cots rfid devices," *IEEE/ACM Transactions on Networking*, vol. 25, no. 6, pp. 3559–3572, 2017.
- [36] J. Wang, L. Chang, O. Abari, and S. Keshav, "Are rfid sensing systems ready for the real world?," in *Proc. ACM MobiSys*, pp. 366–377, 2019.
- [37] L. Yang, Y. Li, Q. Lin, H. Jia, X.-Y. Li, and Y. Liu, "Tagbeat: Sensing mechanical vibration period with cots RFID systems," *IEEE/ACM Transactions on Networking (TON)*, vol. 25, no. 6, pp. 3823–3835, 2017.
- [38] M. Abbak and I. Tekin, "RFID coverage extension using microstrip-patch antenna array," *IEEE Antennas and Propagation Magazine*, vol. 51, no. 1, pp. 185–191, 2009.
- [39] A. M. Ndifon, M. J. Crisp, R. V. Penty, and I. H. White, "Enhanced RFID tag detection accuracy using distributed antenna arrays," in *IEEE International Conference on RFID*, pp. 1–6, 2018.
- [40] Y. Ma, N. Selby, and F. Adib, "Drone relays for battery-free networks," in *Proc. ACM Sigcomm*, pp. 335–347, 2017.
- [41] L. Chen, H. Ba, W. Heitzelmann, and A. Cote, "RFID range extension with low-power wireless edge devices," in *IEEE International Conference on Computing, Networking and Communications*, pp. 524–528, 2013.
- [42] A. J. S. Boaventura and N. Carvalho, "Extending reading range of commercial rfid readers," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 1, pp. 633–640, 2012.
- [43] F. Amato, C. W. Peterson, B. P. Degnan, and G. D. Durgin, "Tunneling rfid tags for long-range and low-power microwave applications," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 2, pp. 93–103, 2018.
- [44] A. Varshney and L. Corneo, "Tunnel emitter: Tunnel diode based low-power carrier emitters for backscatter tags," in *Proc. ACM MobiCom*, pp. 1–14, 2020.
- [45] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "Hitchhike: Practical backscatter using commodity wifi," in *Proc. ACM MobiSys*, pp. 259–271, 2016.
- [46] V. Talla, M. Hesar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, "Lora backscatter: Enabling the vision of ubiquitous connectivity," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 3, p. 105, 2017.
- [47] Y. Peng, L. Shangguan, Y. Hu, Y. Qian, X. Lin, X. Chen, D. Fang, and K. Jamieson, "Plora: a passive long-range data network from ambient lora transmissions," in *Proc. ACM Sigcomm*, pp. 147–160, 2018.