Challenge: RFID Hacking for Fun and Profit

Ju Wang, Omid Abari and Srinivasan Keshav
University of Waterloo
{ju.wang,omid.abari,keshav}@uwaterloo.ca

ABSTRACT

Passive radio frequency identification (RFID) tags are ubiquitous today due to their low cost (a few cents), relatively long communication range (~7-11 m), ease of deployment, lack of battery, and small form factor. Hence, they are an attractive foundation for environmental sensing. Although RFID-based sensors have been studied in the research literature and are also available commercially, manufacturing them has been a technically-challenging task that is typically undertaken only by experienced researchers.

This paper shows how even hobbyists can transform commodity RFID tags into sensors by physically altering ('hacking') them using COTS sensors, a pair of scissors, and clear adhesive tape. Importantly, this requires no change to commercial RFID readers. We also propose a new legacy-compatible tag reading protocol called Differential Minimum Response Threshold (DMRT) that is robust to the changes in an RF environment. To validate our vision, we develop RFID-based sensors for illuminance, temperature, gestures, etc. We believe our approach has the potential to open up the field of batteryless backscatter-based RFID sensing to the research community, making it an exciting area for future work.

CCS CONCEPTS

• **Computer systems organization** → *Sensor networks*;

KEYWORDS

RFID; Modification; Antenna; Sensor

ACM Reference Format:
Ju Wang, Omid Abari and Srinivasan Keshav. 2018. Challenge: RFID Hacking for Fun and Profit. In *Proceedings of 24th Annual International Conference on Mobile Computing and Networking, New Delhi, India, October 29–November 2, 2018 (MobiCom'18),* 10 pages.
https://doi.org/10.1145/3241539.3241561

MobiCom'18, October 29–November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10…$15.00
https://doi.org/10.1145/3241539.3241561

1 INTRODUCTION

Radio frequency identification (RFID) systems have been in widespread use for the last two decades for applications ranging from physical access control to animal husbandry. This is because of their low cost, relatively long communication range, and small form factor [22]. Besides, they are easy to deploy and maintain since they do not require batteries. This makes them attractive as the basis for *wireless and batteryless sensors* [3, 14, 15].

Many researchers have designed RFID tag-based sensors using a variety of approaches.[1] For example, WISP-based tags [12, 15] harvest ambient RF energy and allow a variety of sensors to be interfaced with an on-tag MS430 microcontroller. In contrast, Ekhonet [24] tags use a very low-power ADC and a clock circuit to store sensor readings and respond to an RFID reader. Yang *et al.* [23] design the RFID tags that embed a small amount of distilled water, making their RF response temperature sensitive. However, these approaches require custom tag designs, making tag manufacture out of the reach of most researchers.

Mass-produced RFID tag-based batteryless sensors are also commercially available today. For example, the RFM3200 Wireless Flexible Temperature Sensor from RFMicron Inc. [4] is a batteryless temperature sensor. Similarly, the WISP-like EAL01-Shadow-RM-L108G tag is available from Farsens Inc.[2] However, not only are these tags relatively expensive, researchers cannot extend the functionality of these tags without extensive support from the manufacturer.

In recent work, Pradhan *et al.* [16] show how changes in the received signal due to touching an RFID tag can be used to detect the finger gestures of touches or swipes. Our work advances this idea. Specifically, we show how *physical modifications* to a commodity tag allow it to sense any environmental variable that can be translated into a variation in resistance. For instance, by suitably integrating a phototransistor or a thermistor into a commodity RFID tag, we can convert it into the light or temperature sensor. We also propose and evaluate a new legacy-compatible tag reading protocol called Differential Minimum Response Threshold (DMRT) that is robust to the changes in the RF environment.

[1] We discuss a few representative designs here, deferring more details to Section 5.
[2] http://www.farsens.com/en/products/eval01-shadow-rm-l108g/

Our approach allows even high-school students to build their own batteryless wireless RFID sensors, opening this area for future innovations. This has promising implications for cyber-physical systems of tomorrow.

This paper makes the following contributions:

- We show how to trivially modify commodity RFID tags to convert them into environmental sensors.
- We propose and evaluate a new legacy-compatible tag reading protocol that we call Differential Minimum Response Threshold.
- We demonstrate the value of our approach by creating RFID-based contact, light and temperature sensors.

Paper outline: We introduce the background in Section 2 and detail our design in Section 3. Some applications enabled by our work are described in Section 4, followed by the related work in Section 5. We discuss challenges and limitations in Section 6 and conclude the paper in Section 7.

2 BACKGROUND

2.1 Active and Passive RFID Tags

RFID tags evolved from product barcodes, allowing readers to use RF signal rather than optics to read up to about 2 KB of on-tag data [22]. This data can be read-only, read-write, or write-once-read-many.

Many types of RFID tags are in common use today. A useful distinction to make is between *active* and *passive* tags. Active tags have their own power source and can have a range as high as 500 m [10]. However, they need an on-tag battery and can be relatively expensive. In contrast, passive tags are batteryless, being powered by inductive coupling with RF energy generated by a reader, which also serves as the communication peer. This also makes them much lower-cost, though with a lower communication range.

Passive tags can use either the *near field* or the *far field* power communication. With the near-field communication, tags need to be within about 1 cm of the reader. In contrast, with the far-field communication, tags can be up to ~7-11 m away, and communication is by *backscatter*, i.e., modification of the antenna's impedance by the RFID tag's chip. A reader transmits an RF signal as a query. Nearby tags use this query to power up and respond their unique ID using ON-OFF keying modulation. The tags transmit a '1' bit by changing their internal impedance to reflect the reader's signal and a '0' bit by not reflecting the signal.

Backscatter communication has been widely studied in recent years (see References [13, 19] for two recent surveys). We build on this body of work, using RFID backscatter communication as the basis for sensing.

Figure 1 shows a typical passive RFID tag, which has two main parts:

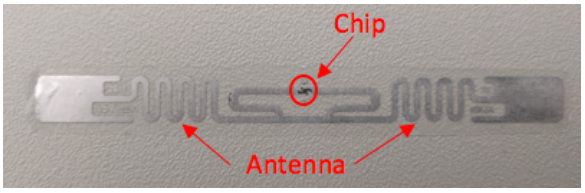


Figure 1: Alien Squiggle general purpose RFID tag.

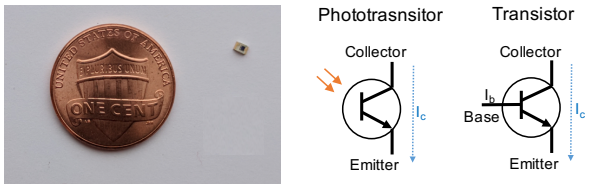


Figure 2: (a) A phototransistor used in our experiments, and (b) the block diagrams of phototransistors and transistors.

- an antenna which receives and also reflects the RFID reader's signal.
- a chip which includes power harvesting circuits, logic and memory units, and a switch to change the impedance of the antenna.

For an RFID tag to respond to a reader's query, the tag's antenna must receive and deliver sufficient power to the tag's chip. Therefore, the minimum amount of power required to read a tag depends to the amount of power that a tag's antenna receives (a function of the RF environment and the tag-reader distance) and the percentage of the power that the tag's antenna passes to its chip.

2.2 Phototransistors

A phototransistor is a light-sensitive transistor [17]. Figure 2 shows a phototransistor and its block diagram. In contrast to transistors, phototransistors' currents are controlled by the amount of light they get exposed to. Therefore, one can use a phototransistor as a switch or a variable resistor where its value changes depending on the amount of light they get exposed to. Phototransistors cost 5-10 US cents [7].

2.3 Thermistors

A thermistor is a temperature-sensitive resistor (Figure 3). In contrast to resistors, the resistance of a thermistor depends on its temperature. There are two types of thermistors: NTC (negative temperature coefficient) and PTC (positive temperature coefficient). When the temperature increase, the resistance of NTC thermistors decreases, while the resistance of PTC thermistors increases. Thermistors are also inexpensive, which cost 10-50 US cents for each [8].

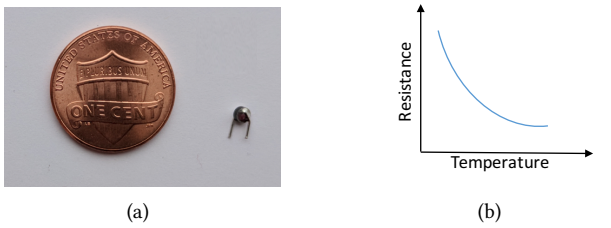


Figure 3: (a) An NTC thermistor used in our experiments, and (b) its functionality.

3 OUR APPROACH

In this section, we present our approach of modifying passive RFID tags. We first explain how to modify a tag (Section 3.1), then perform some experiments to find the best place of the tag antenna for the modification (Section 3.2). Next, we introduce DMRT, a new legacy-compatible tag reading protocol to query the modified tags (Section 3.3). Finally, in Section 3.4 we discuss how to choose sensors that are compatible with our approach.

3.1 Tag Modification

As explained in Section 2, the resistance of a phototransistor or a thermistor changes due to the change of light or temperature, respectively. This change in resistance can be used to progressively detune the tag's antenna. Thus, our key idea is to cut away a small part of the tag's antenna, breaking the antenna's circuit, and replacing the cut section with a sensor.

Figure 4 shows the steps to modify an RFID tag. We first remove the plastic cover on the tag to expose the antenna, which is a thin metallic strip on a plastic base. Next, we cut away a small part of its antenna. Finally, we place a sensor such as a phototransistor or a thermistor to replace the cut part and secure it on the tag using the clear plastic tape.

Our hypothesis is that as the light or temperature changes, this affects the resistance of the sensor, and hence the antenna's properties also will change. This should be detectable at the reader as a change in the received signal strength (RSS) or the phase of the reflected RFID signal. Therefore, we should be able to estimate the sensor's value by monitoring these signal changes.

3.2 Where to Modify A Tag?

Tag modification can be done at one of the numerous locations on the tag's antenna: which location is the best? Our intuition is that the closer we place a sensor to the tag's chip, the greater the impact on RSS and phase changes of the reflection signal. To evaluate this intuition, we place three

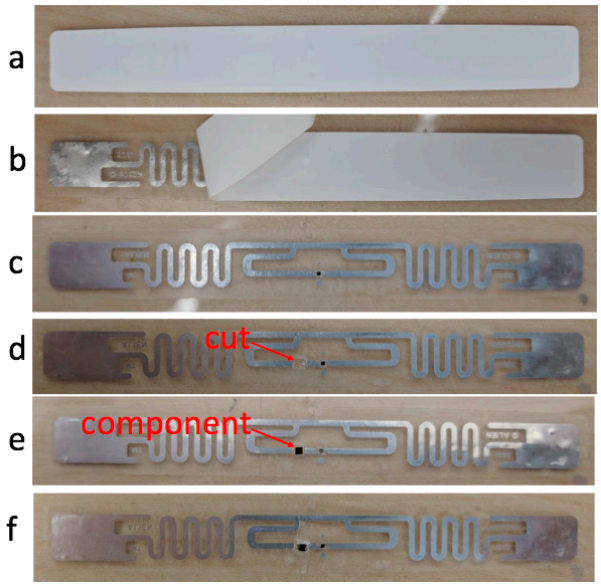


Figure 4: How we modify a tag: (a) we use a commodity RFID tag, (b,c) remove the plastic cover, (d) cut away a small part of its antenna, (e) replace it with a sensor component, and (f) secure it using tape.

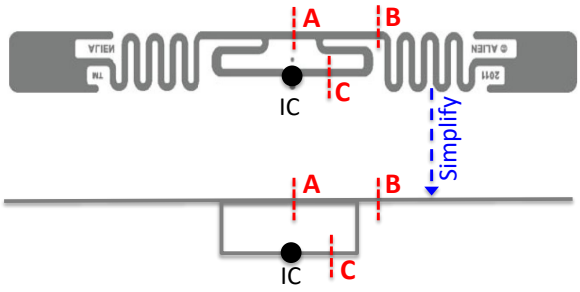


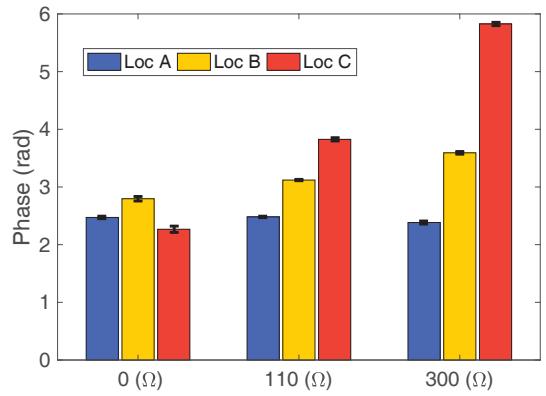
Figure 5: Three potential cutting locations on a tag.

tags at a distance of 1 m from the reader. We cut different locations on each tag, as shown in Figure 5, replacing each cut portion with an SMD (Surface-Mount Device) resistor. We then measure the phase and RSS at the reader for different resistor values.

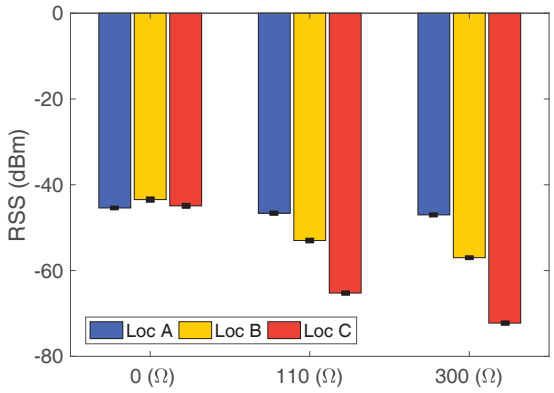
Figure 6 plots the RSS and phase for different values of resistors and different cut locations. We see that for the same amount of change in the resistance, the tag cut at 'Location C' has the largest change in its phase and RSS: the phase changed by more than 3.5 radians and the RSS has changed by 25 dB. Therefore, we recommend placing sensors at the 'Location C', which is the closest to the tag's chip.

3.3 The DMRT Tag Reading Protocol

We now discuss how to read sensor values from a modified tag. This aims to finding a signal feature that is impacted by



(a) Phase readings.



(b) RSS readings.

Figure 6: (a) Phase and (b) RSS versus resistor values for the three tags. Each tag has a resistor placed at a different location. The figure shows that placing the component on 'Location C' has the greatest impact on the phase and RSS values of the RFID signal.

the sensor reading, and is also robust to the changes in the RF environment. We first explain our differential sensing approach in Section 3.3.1, then introduce a novel signal feature we call *differential minimum response threshold* or *DMRT* in Section 3.3.2.

3.3.1 Differential Sensing. In prior work, changes in the phase and RSS readings of a tag's signal have been used for tasks such as localization [21], gesture sensing [16] and material sensing [20]. However, it is well known that neither of them are robust to the changes in the RF environment. For example, the phase and RSS readings suffer from a large variation when a moving object (e.g., person) blocks the Line of Sight (LoS) path between a tag and the reader's antenna, or when the location of a tag or the reader changes. This makes it impossible to use the absolute value of RSS or phase

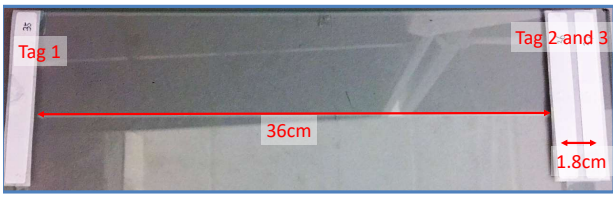


Figure 7: Experiment layout for testing the differential sensing.

change to 'read' a sensor since we cannot distinguish between a change due to a sensor and a change due to the RF environment.

To solve this problem, we use differential sensing, i.e., we measure the impact of a sensor on one of two closely-spaced tags' feature (e.g., phase/RSS) values, instead of a single tag's absolute feature value. Intuitively, two closely-spaced tags have nearly the same channel to and from the RFID reader. Thus, we can remove the phase/RSS variations caused by the RF environment by measuring the difference in the feature values of the two tags.

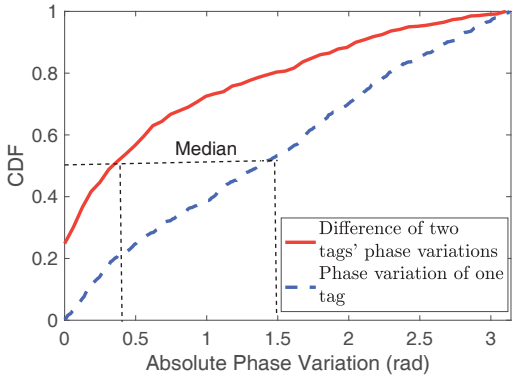
We now present experimental evidence to support our claim that the differential sensing is more stable than using the absolute feature values. Specifically, we show that the phase/RSS of a single tag varies significantly, but the phase/RSS difference of two closely placed tags is relatively stable.[3]

In an indoor environment, we deploy an RFID reader (Impinj R420 reader [9]), and three identical tags as shown in Figure 7. 'Tags 2 and 3' are 1.8 cm apart, but 'Tag 1' is placed 36 cm away from these two tags.[4] The distance between the reader's antenna and the tags is 2.8 m. To create multipath and change the environment, we let a person move around the area between the antenna and the tags while the LoS is always blocked. The phase and RSS readings of closely placed tags, i.e., 'Tags 2 and 3', are used in differential processing, while the phase and RSS readings of a single tag, i.e., 'Tag 1', is used for comparison.

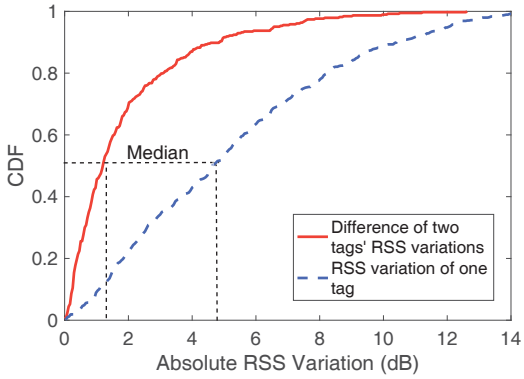
Figure 8 shows the CDF of the absolute phase and RSS variations of a single tag and, differential phase and RSS variations of two tags. Due to the dynamic environment, the absolute phase variation of one tag is uniformly distributed $[0, \pi]$, and with a median variation as large as 1.5 radians. However, the median variation of the phase difference of two closely deployed tags is only 0.4 radians. The variation of the RSS measurement is also reduced by using the differential method. Specifically, the median RSS variation is reduced from 5 dB to 1.8 dB by using the differential method.

[3]In fact, even with differential sensing, these feature values turn out to be insufficiently stable, which motivates the design of the DMRT feature, presented in Section 3.3.2.

[4]There is no coupling effect between 'Tag 1' and 'Tags 2-3', given the 36 cm distance.

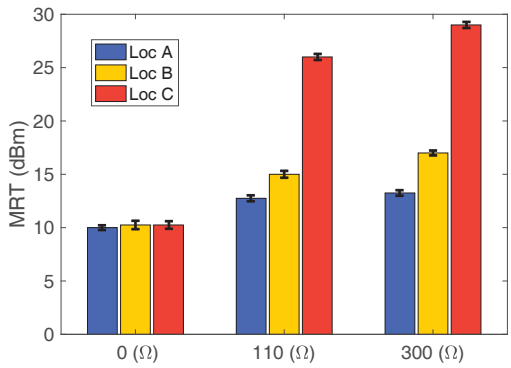


(a) Phase variations.

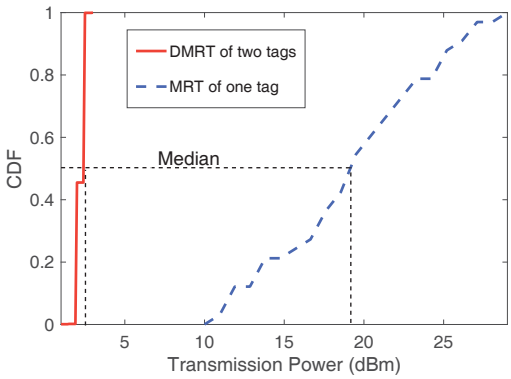


(b) RSS variations.

Figure 8: CDF of (a) phase variations and (b) RSS variations in a dynamic RF environment. The dashed blue line shows the variations in absolute value and the solid red line shows the variations relative to a reference tag. Using a reference tag reduces the impact of the changes in the RF environment on the RSS and phase readings.



(a) Changes in MRT versus resistor values and cutting locations.



(b) Comparsion of MRT and DMRT in a dynamic environment.

Figure 9: Required minimum response threshold (MRT) to activate a tag: (a) Changes in MRT when changing the resistor values and the cutting locations, (b) CDF of MRT and DMRT in a dynamic environment. The dashed blue line shows the variations in the absolute value and the solid red line shows the variations relative to a reference tag.

3.3.2 Differential Minimum Response Threshold. Although we find that the variations of the phase/RSS readings are reduced by using the differential measurements, the 80% variations of the differential phase and RSS are still quite high: 1.4 radians and 4 dB in Figure 8, respectively. Hence, we introduce a new signal feature–*minimum response threshold* (MRT)–defined as the required minimum transmission power of the reader to activate a tag. The MRT is determined by gradually increasing the RFID reader's transmission power from 10 dBm to 32.5 dBm with a step of 0.25 dBm and recording the minimum transmission power required to makes the tag readable (i.e., the reader receives 5-7 packets per second from the tag).[5] We also define *differential MRT* as the difference in transmission power required to active a modified tag, when compared to a co-located unmodified tag.[6]

Although we have shown that the 'Location C' on a tag is the best location for measuring the changes in RSS or phase due to a sensor, it is not obvious that this is also the best location when using the DMRT. Hence, using an experimental approach identical to that in Section 3.2, we obtain the results in Figure 9 (a). These results validate that the 'Location C' is

[5]Changing a reader's transmission power is an available feature in commodity RFID readers.

[6]The coupling between two co-located tags does not affect the sensing accuracy for two reasons: (i) the coupling effect will not change over time; (ii) DMRT is a differential scheme, which will remove the coupling effect between two tags.

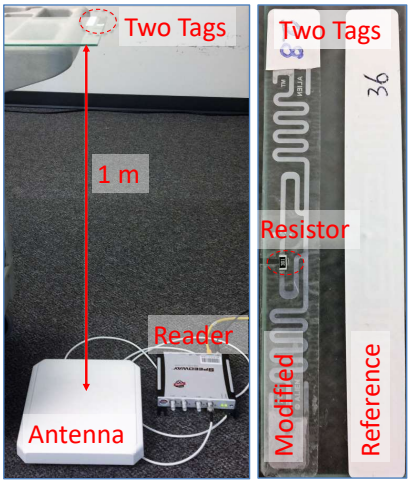


Figure 10: Experimental setup of measuring DMRT for different resistor values.

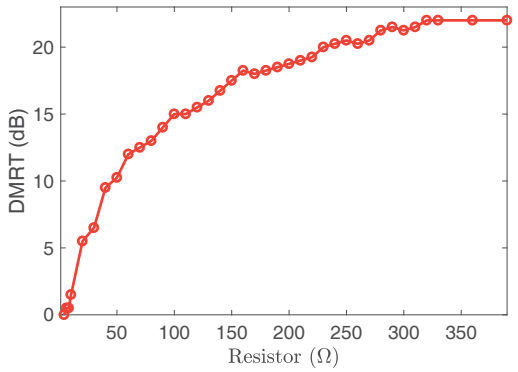


Figure 11: DMRT versus the values of a resistor mounted on the tag.

also the best location for measuring the MRT. We use this location for placing sensors in the remainder of this paper.

Next, we show through real-world experiments that DMRT is robust to the changes in the RF environment, caused by moving people or changes in the tags' locations. In the indoor environment, we randomly choose 11 different locations to co-deploy a modified tag and a reference tag, as in Section 3.3.1. Figure 9 (b) shows the MRT for activating a single tag as well as the DMRT. It is obvious that although the MRT of a single tag varies a lot, the DMRT metric is very stable, with a 90% variation of less than 2.5 dB. Given that the DMRT is nearly independent of tags' locations and also robust to the changes in the RF environment, we recommend this approach for reading modified RFID tags.

3.4 Sensor Selection

There are many different types of photodiodes and thermistors available in the market with different impedance ranges. We now provide some guidelines on sensor selection, based on our experiments.

Specifically, we deploy two tags at fixed locations, as shown in Figure 10. The tags are closely deployed with a distance of 1.8 cm. One tag serves as a reference and the other one is modified with a resistor. The distance between the tags and the reader's antenna is 1 m. We then measure the DMRT for different resistor values, ranging from 2 Ω to 390 Ω.[7]

Figure 11 shows the DMRT as a function of the resistor values. It is clear that DMRT does not vary much for resistor values larger than 250 Ω. Therefore, we recommend that sensor resistor values vary in the range from 0 Ω to 250 Ω as a function of the environmental variable being sensed.

To summarize, our approach is to (i) selecting sensors whose resistance varies from 0 Ω to 250 Ω (ii) modifying commodity passive RFID tags by cutting their antenna at 'Location C' and taping on a sensor and (iii) reading the sensor value by using the DMRT feature. Next, we will show how our approach can be used to create a variety of interesting and useful sensors.

4 APPLICATIONS

This section discusses some preliminary results using our approach to create novel RFID-based sensors.

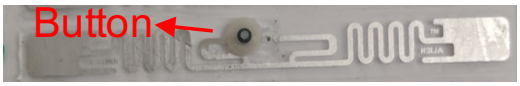
4.1 Keypad

Perhaps the easiest way to modify a tag is to cut away a portion of the antenna, completing the antenna circuit only when a button is pressed. We use this approach to create a low-cost batteryless and wireless keypad. Our keypad consists simply of an array of tags mounted on a surface. Each tag is modified by cutting away a small part of its antenna and placing a silicone button on it, as shown in Figure 12. In the default mode, no tag's respond. However, when a button is pushed, only the corresponding tag's antenna is activated and the tag will respond. Therefore, the reader can detect which button has been pushed by the user. This approach allows simultaneous button pushes on multiple tags, since a reader can read multiple tags at almost the same time.

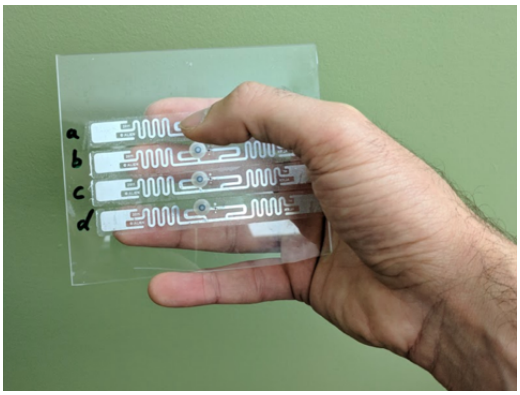
4.2 Temperature Sensing

As discussed in Section 2, we use a thermistor (i.e., a temperature-sensitive resistor) as our temperature sensor. To use DMRT, we use co-locate two tags: one serves as a reference and the

[7] The resistor values change with a step of 2 Ω from 2 Ω to 10 Ω, and a step of 10 Ω from 10 Ω to 330 Ω.



(a)



(b)

Figure 12: (a) A tag is modified by cutting away a small part of its antenna and placing a silicone button on it. (b) Our keypad consists of an array of tags mounted on a surface.

other one is modified with a thermistor. To evaluate the sensor performance, we perform measurements for 15 different tag locations in our lab and at different temperature values.

Figure 13 shows the result of this experiment. The figure shows a clear relation between DMRT and temperature. Specifically, as temperature increases, DMRT decreases. This is due to the fact that the resistance of the thermistor decreases with temperature increases, and therefore a large percentage of received power is passed to the chip. It implies that one can estimate the temperature of the tag by measuring DMRT at the reader side.

Note that even with an approximately 10 °C change in the temperature, the confidence intervals of adjacent columns on the histograms overlap. This indicates that the sensor has quite coarse sensitivity, with a least count of about 20 °C. We hope to address this limitation in the future work.

4.3 Light Sensing

For light sensing, we use a phototransistor (i.e., a light-sensitive switch) as our light sensor, rather than photoresistors. This is because photoresistors are designed to operate in a DC (Direct Current) environment, but placing them on an RFID tag requires them to operate at 900 MHz. This creates a new problem: photoresistors have an unwanted parasitic capacitance (in the range of a few nF) in parallel with their variable resistor. Therefore, when they are coupled with an

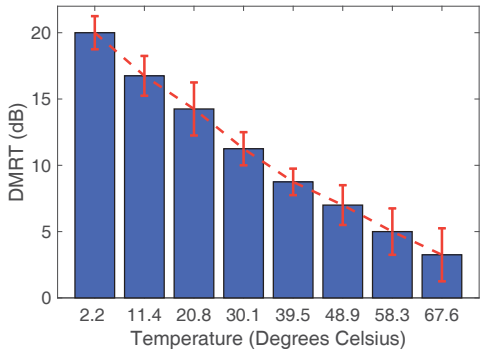


Figure 13: DMRT over different temperatures. DRMT decreases as the temperature increases.

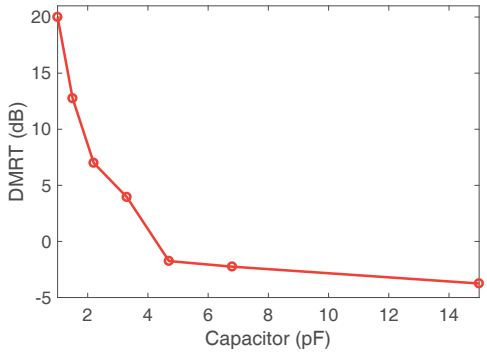


Figure 14: DMRT versus different capacitor values.

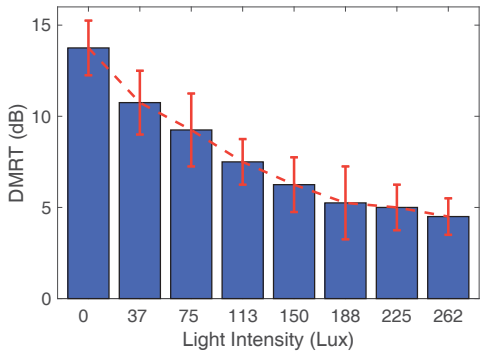


Figure 15: DMRT versus light intensity. DMRT decreases as the light intensity increases. The reader can measure DMRT and therefore estimate the illuminance at the tag's location.

RF signal in the 900 MHz range, they act as a short circuit, i.e., zero resistance, making them useless as sensors.

To deal with this, we sense light using phototransistors rather than photoresistors. We experimentally determine

that for typical phototransistors, the parasitic capacitance is much smaller than for photoresistors (in the range of sub pF), and therefore they do not short circuit the phototransistor. Moreover, their capacitance increases as the light intensity increases. Therefore, the impedance of a phototransistor varies with the intensity of light.

To choose the right phototransistor value, similar to our experiments in Section 3.4, we run experiments where we placed different capacitors instead of resistors on a modified RFID tag. Figure 14 shows the results of DMRT versus different capacitor values. It is clear from the figure that the value of DMRT does not vary much for a capacitance larger than 10 pF. Therefore we should pick a phototransistor whose parasitic capacitance changes from 0 pF to 10 pF across the desired illuminance measurement range.[8]

With this choice of phototransistors, our approach successfully measures light levels, as shown in Figure 15. We see that the light intensity increases from 0-260 Lux (a typical work surface has an illuminance of 300 Lux), the DMRT decreases nearly linearly. As with temperature sensing, however, it is clear that the confidence intervals of the adjacent columns overlap, so the granularity of this sensor is quite coarse: about 75 Lux.

4.4 Gesture Sensing

As a more advanced demonstration of the power of our approach, we show how to use RFID sensors to detect a simple 'wave' gesture over an array of sensors (Figure 16). To do so, we place multiple light sensors on a surface. Then, as a user moves his hand over the surface, the reader reads DMRT of all sensors.

Figure 17 shows the DMRT versus hand positions for all sensors. It is clear that DMRT significantly increases when the hand blocks the light to a sensor. Therefore, we can use this approach to detect the location of the hand within an accuracy of a few centimetres. Note that, the accuracy can be further improved by placing tags closer to each other. Moreover, placing the tags in a 2D pattern would allow more sophisticated gestures to be recognized.

4.5 Other Sensors

We now describe some other sensors enabled by our approach:

- **Door open sensor:** A door open/close sensor is a simple extension of the keypad sensor. When a door is closed, it closes the switch, allowing the RFID tag to be read, and when it is open, the RFID tag cannot be read. This type of sensor would be important in home security applications.
- **Colour sensor:** A pair of modified tags can be used as a colour sensor by covering one of the phototransistors with a colour filter. For example, to detect red light, one of the phototransistors would need to be covered with a red filter. If the ambient light were fully red, then both phototransistors would have the same DMRT value. Any deviation from redness would reduce the filtered phototransistor's DMRT value compared to the other phototransistor. Thus, this can be interpreted as light having less redness. By extending this approach to other colour filters, it is possible to build a batteryless colour sensor.
- **Humidity sensor:** Commercially-available humidity sensors translate a change in humidity to a change in resistance. This can easily be detected by using our approach.
- **Pressure sensor:** Similar to humidity sensors, pressure sensors change their impedance with a change in pressure, allowing them to be integrated into modified RFID tags by using our approach.

[8] In our experiments, we use a phototransistor (OSRAM SFH 3710) whose parasitic capacitance changes from 0 pF to ~100 pF. Therefore, we place a 10 pF capacitor in series with the phototransistor to limit its range from 0 pF to 10 pF.

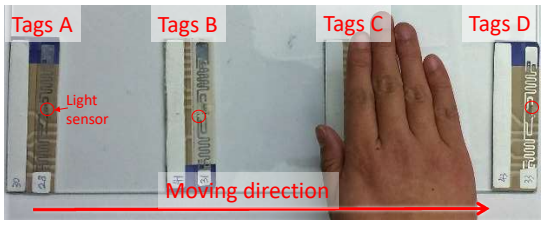


Figure 16: Hand gesture sensing.

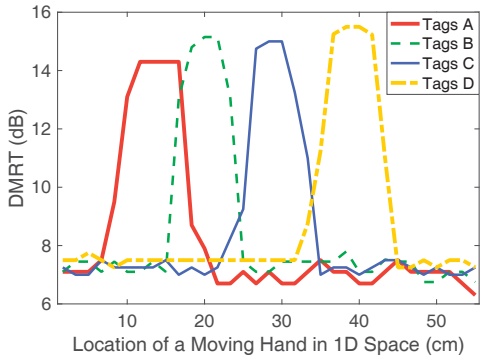


Figure 17: DMRT versus hand positions for all sensors. DMRT significantly increases when the hand blocks the light to a sensor.

5 RELATED WORK

Many researchers have designed RFID tag-based sensors. Following Marrocco, one way to categorize this work is along

two axes: whether the tag is self-sensing or there is a specific sensor and whether the data transmission mode is analog or digital [14].

With self-sensing tags, the RF response of the tags depends on environmental parameters, allowing them to act as sensors. For example, in work by Capdevila *et al.*, the water level in a container is detected by attaching multiple tags to the container: as the water level rises, each tag in turn makes an OFF-ON transition [3]. Similarly, in work by Pradhan *et al.*, changes in backscatter phase due to touching or swiping a tag are used to detect these motions [16]. Some recent papers [5, 11] also demonstrate the sensing of human-object interaction by using Wi-Fi backscatter signals. Self-sensing tags are generally limited in what they can sense, since the environmental condition must somehow be coupled to detectable RF parameters.

Other tags incorporate specific sensors. For example, Yang *et al.* [23] design RFID tags that embed a small amount of distilled water, making their RF response temperature sensitive. Similarly, Shi *et al.* [18] use a bimetallic strip to torque a tag's antenna to change its resonant frequency. These and related approaches, such as in References [2, 6], require custom tag designs, making them relatively expensive, and inaccessible to most researchers. Our work incorporates specific sensors, but is accessible to most researchers.

Some tags use analog mode transmission, that is, their RF response is modified in some way by the sensed variable. The examples so far all fall into this category. In contrast, with digital mode transmission, the sensed parameter is stored on the tag, then read later from the tag's on-chip memory (see [1] for a recent survey). Examples include the RFM3200 Wireless Flexible Temperature Sensor from RFMicron Inc. [4], WISPs [15] and Ekhonet [24]. The need for writing into on-tag memory increases the cost of the tags as well as that of the readers. For example, temperature-sensing tags from RFMicron cost about 3 USD. In contrast, our approach modifies inexpensive passive RFID tags that cost about 0.03∼0.05 USD each, which is a reduction in cost by two orders of magnitude. Moreover, we can use standard RFID readers, rather than the more expensive RAIN/UHF RFID readers.

Our work can be classified as a 'tag with a specific sensor and analog communication'. It differs from prior work in that we physically modify a tag to add sensing capabilities (but with low added cost). Moreover, we introduce the concept of minimum response threshold and differential sensing to improve the robustness of our approach.

6 CHALLENGES AND DISCUSSION

Our work is not without some significant limitations. Here, we discuss these limitations and the corresponding challenges for researchers in this field.

Improving the sensing accuracy. The values sensed by using our approach are somewhat coarse-grained. This is to be expected, given our dependence on the volatile RF measurements to extract sensor values. One approach to improving the sensing accuracy would be to improve the resolution of DMRT. Currently, the resolution of DMRT in our implementation is 0.25 dBm, a limitation of our reader. To improve this resolution, one can design or use a reader which has finer granularity for changing transmission power. Second, we need to identify sensors that consistently detune RFID antennas when exposed to changes in the environment. To do so, it requires understanding and quantifying the impact of a sensor on antenna characteristics, such as matching, polarization, beam patterns, and S-parameters.

Improving the sensing range. Tag modifications necessarily reduce its range. An unmodified tag has a range of ∼7-11 m, but modified tags have a range that is only about 4 m. To improve the tag's reading range, the sensor should not significantly detune the antenna gain and sensitivity. One way to achieve this is by using a rigorous tag antenna model to model cutting and placing a sensor on the tag antenna. Alternatively, one can design a compensation scheme to ensure the impedance match between the sensor and the tag antenna.

Real-time DMRT estimation. In our current implementation, it takes ∼0.1-7.2 s to estimate DMRT, since each transmission power can be changed only every 0.1 s when sweeping power. This limitation of the reader hardware makes it difficult to track a fast-moving gesture. To solve this issue, the challenge is to design a reader that can sweep the transmission power more quickly.

Removing the parasitic capacitance. Parasitic capacitance is an unwanted capacitance that exists in many sensors. Given the 900 MHz RFID signal, even a parasitic capacitance of a few pF can result in the sensor's impedance exceeding the target range or potentially short circuit the sensor. To solve this problem, we place an additional small capacitor in series with the sensor to limit its impedance. However, this can reduce the sensor's accuracy. Alternatively, it is possible to cancel the parasitic capacitance by putting an appropriate inductor in parallel with the sensor. This inductor, of the order of a few nH, must be chosen with care. Modifying RFID tags while mitigating the effect of parasitic capacitance is, therefore, a fruitful area for future work.

Dealing with the tag diversity. Due to the tag diversity, different types of tags may have different DMRT values even in the same environment (e.g., same light intensity). One way to solve this problem would be to transform DMRT readings from different tag types into a uniform space, so that all tags show a consistent sensing result in the transformed space. That is to say, in the transformed space, all different tags will show a same sensing result for the same environment.

Reducing the reader cost. Although the passive RFID tags are inexpensive, readers are not: a typical RFID reader costs between ~100-500 USD. Therefore, designing a low-cost RFID reader is still a challenge in existing RFID-based applications.

We hope that our future work, as well as that from others in this field, will address these important challenges.

7 CONCLUSION

This paper discusses how to use simple modifications of commodity RFID tags to turn them into batteryless, wireless, low-cost sensors. Unlike prior work, which required complex tag designs, our approach is suitable for use even by novice researchers. Moreover, we have used experiments to determine (i) the best location to modify a tag (ii) the sensor impedance range compatible with our approach. We have also designed and implemented the DMRT approach to query sensor values in a way that is robust to the changes in the RF environment. Finally, we have used our approach to design and test tags for sensing of light, temperature, touch, and gesture.

In summary, our work demolishes the myth that RFID-sensing tags can only be designed by a handful of experienced researchers. Instead, we have presented a novel and exciting approach to design and implement RFID-based sensing that opens up this area to even novice researchers. We look forward to exploiting this approach in a new generation of cyber-physical systems.

ACKNOWLEDGMENT

We would like to thank the shepherd and the anonymous reviewers for their valuable feedback on this paper. We also thank Costin Ograda-Bratu for his help with the experiments.

REFERENCES

[1] Teemu Ainasoja. 2018. Sensors, Healthcare IoT and Pigeon Races - Review of RAIN RFID Research. (March 2018). Retrieved June 27, 2017 from http://voyantic.com/blog/posts/sensors-healthcare-iot-and-pigeon-races-review-of-rain-rfid-research-in-2017

[2] Daniel Alonso, Qianyun Zhang, Yue Gao, and Daniel Valderas. 2017. UHF passive RFID-based sensor-less system to detect humidity for irrigation monitoring. *Microwave and Optical Technology Letters* 59, 7 (2017), 1709–1715.

[3] Santiago Capdevila, Lluis Jofre, Jordi Romeu, and Jean-Charles Bolomey. 2011. Passive RFID based sensing. In *Proc. IEEE International Conference on RFID-Technologies and Applications*. 507–512.

[4] RFMicron Corp. 2018. RFM3200 Wireless Flexible Temperature Sensor. (March 2018). Retrieved June 27, 2017 from http://rfmicron.com/rfm3200-wireless-flexible-temperature-sensor/

[5] Chuhan Gao, Yilong Li, and Xinyu Zhang. 2018. LiveTag: Sensing Human-Object Interaction through Passive Chipless WiFi Tags. In *Proc. USENIX NSDI*. 533–546.

[6] Xianjun Huang, Ting Leng, Thanasis Georgiou, Jijo Abraham, Rahul Raveendran Nair, Kostya S Novoselov, and Zhirun Hu. 2018. Graphene oxide dielectric permittivity at GHz and its applications for wireless humidity sensing. *Scientific reports* 8, 1 (2018), 43.

[7] Digikey Inc. 2016. Phototransistors. (March 2016). Retrieved June 20, 2018 from https://www.digikey.com/products/en/sensors-transducers/optical-sensors-phototransistors/544

[8] Digikey Inc. 2017. Thermistors. (July 2017). Retrieved June 20, 2018 from https://www.digikey.com/products/en/sensors-transducers/temperature-sensors-ntc-thermistors/508

[9] Impinj Inc. 2010. R420 Readers. (mar 2010). Retrieved June 27, 2017 from http://www.Impinj.com/products/readers/

[10] SkyRFID Inc. 2018. RFID Tag Maximum Read Distance. (March 2018). Retrieved June 27, 2017 from http://www.skyrfid.com/RFID_Tag_Read_Ranges.php

[11] Vikram Iyer, Justin Chan, and Shyamnath Gollakota. 2017. 3D printing wireless connected objects. *ACM Transactions on Graphics (TOG)* 36, 6 (2017), 242–251.

[12] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. 2013. Ambient backscatter: wireless communication out of thin air. In *ACM SIGCOMM Computer Communication Review*, Vol. 43. 39–50.

[13] Xiao Lu, Dusit Niyato, Hai Jiang, Dong In Kim, Yong Xiao, and Zhu Han. 2017. Ambient Backscatter Networking: A Novel Paradigm to Assist Wireless Powered Communications. *arXiv preprint arXiv:1709.09615* (2017).

[14] Gaetano Marrocco. 2010. Pervasive electromagnetics: Sensing paradigms by passive RFID technology. *IEEE Wireless Communications* 17, 6 (2010), 10–17.

[15] Matthai Philipose, Joshua R Smith, Bing Jiang, Alexander Mamishev, Sumit Roy, and Kishore Sundara-Rajan. 2005. Battery-free wireless identification and sensing. *IEEE Pervasive computing* 4, 1 (2005), 37–45.

[16] Swadhin Pradhan, Eugene Chai, Karthikeyan Sundaresan, Lili Qiu, Mohammad A Khojastepour, and Sampath Rangarajan. 2017. RIO: A Pervasive RFID-based Touch Gesture Interface. In *Proc. ACM MobiCom*. 261–274.

[17] Radio-Electronics.com. 2018. Phototransistor Tutorial. (March 2018). Retrieved June 27, 2017 from https://preview.tinyurl.com/7yy5lak

[18] Xianwei Shi, Fan Yang, Shenheng Xu, and Maokun Li. 2017. A Passive Temperature-Sensing Antenna Based on a Bimetal Strip Coil. *Sensors* 17, 4 (2017), 665–672.

[19] Nguyen Van Huynh, Dinh Thai Hoang, Xiao Lu, Dusit Niyato, Ping Wang, and Dong In Kim. 2017. Ambient Backscatter Communications: A Contemporary Survey. *arXiv preprint arXiv:1712.04804* (2017).

[20] Ju Wang, Jie Xiong, Xiaojiang Chen, Hongbo Jiang, Rajesh Krishna Balan, and Dingyi Fang. 2017. TagScan: Simultaneous target imaging and material identification with commodity RFID devices. In *Proc. ACM MobiCom*. 288–300.

[21] Ju Wang, Jie Xiong, Hongbo Jiang, Xiaojiang Chen, and Dingyi Fang. 2017. D-Watch: Embracing 'Bad' Multipaths for Device-Free Localization With COTS RFID Devices. *IEEE/ACM Transactions on Networking* 25, 6 (2017), 3559–3572.

[22] Roy Want. 2006. An introduction to RFID technology. *IEEE Pervasive Computing* 5, 1 (2006), 25–33.

[23] Fan Yang, Qian Qiao, Juha Virtanen, Atef Z Elsherbeni, Leena Ukkonen, and Lauri Sydanheimo. 2012. Reconfigurable sensing antenna: A slotted patch design with temperature sensation. *IEEE Antennas and Wireless Propagation Letters* 11 (2012), 632–635.

[24] Pengyu Zhang, Pan Hu, Vijay Pasikanti, and Deepak Ganesan. 2014. Ekhonet: High speed ultra low-power backscatter for next generation sensors. In *Proc. ACM MobiCom*. 557–568.