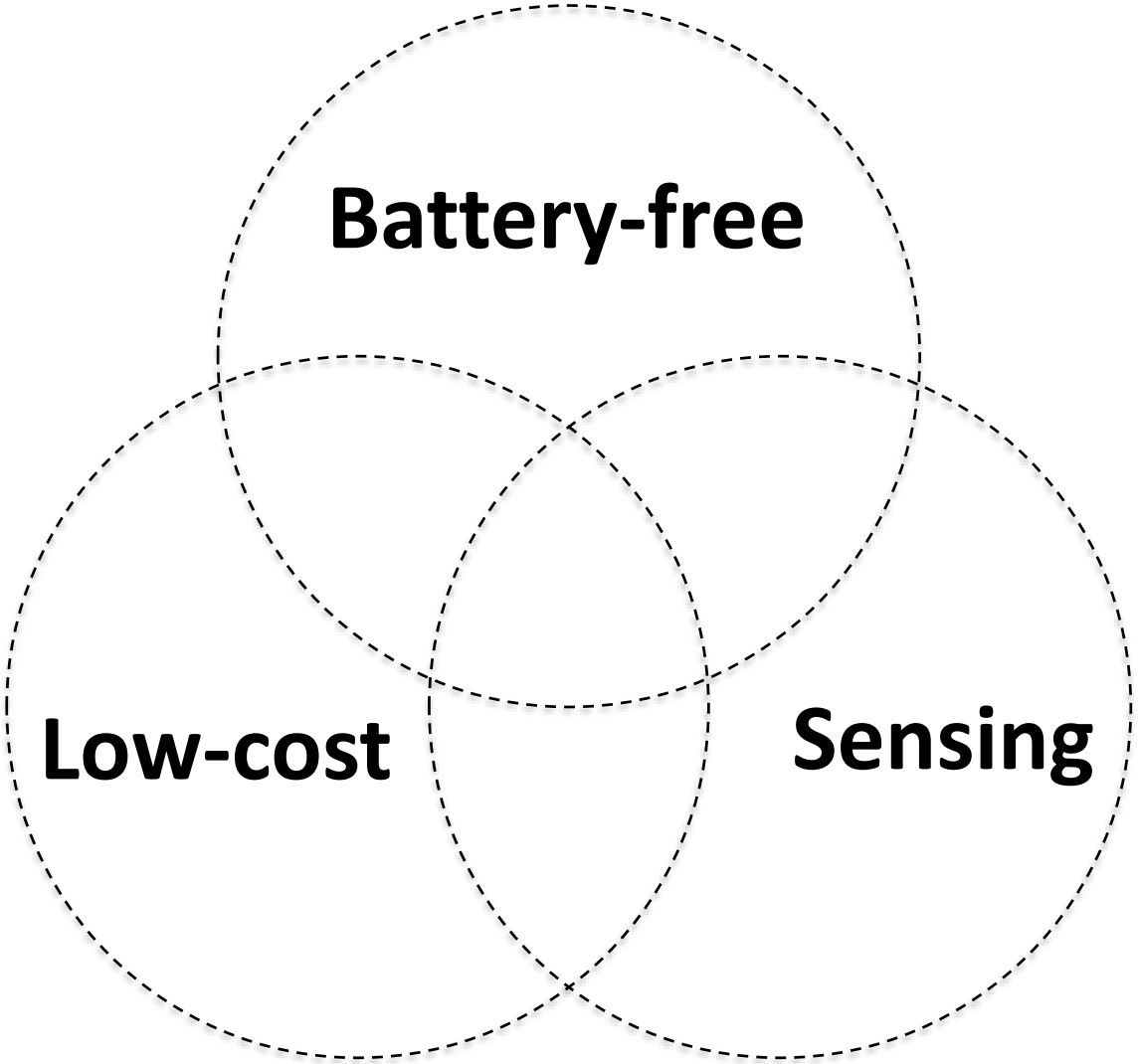
MobiCom 2018, New Delhi, India

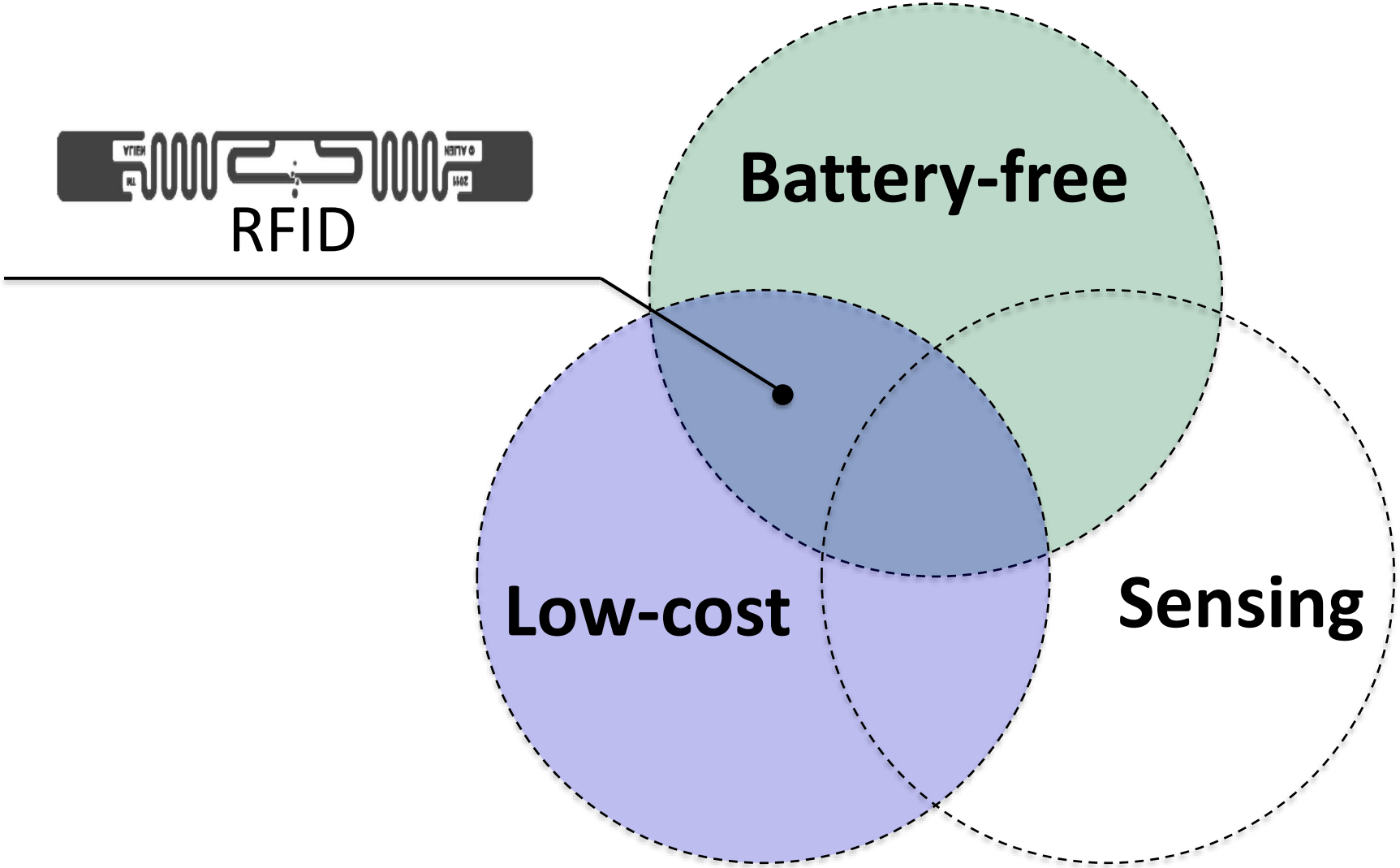
Challenge: RFID Hacking for Fun and Profit

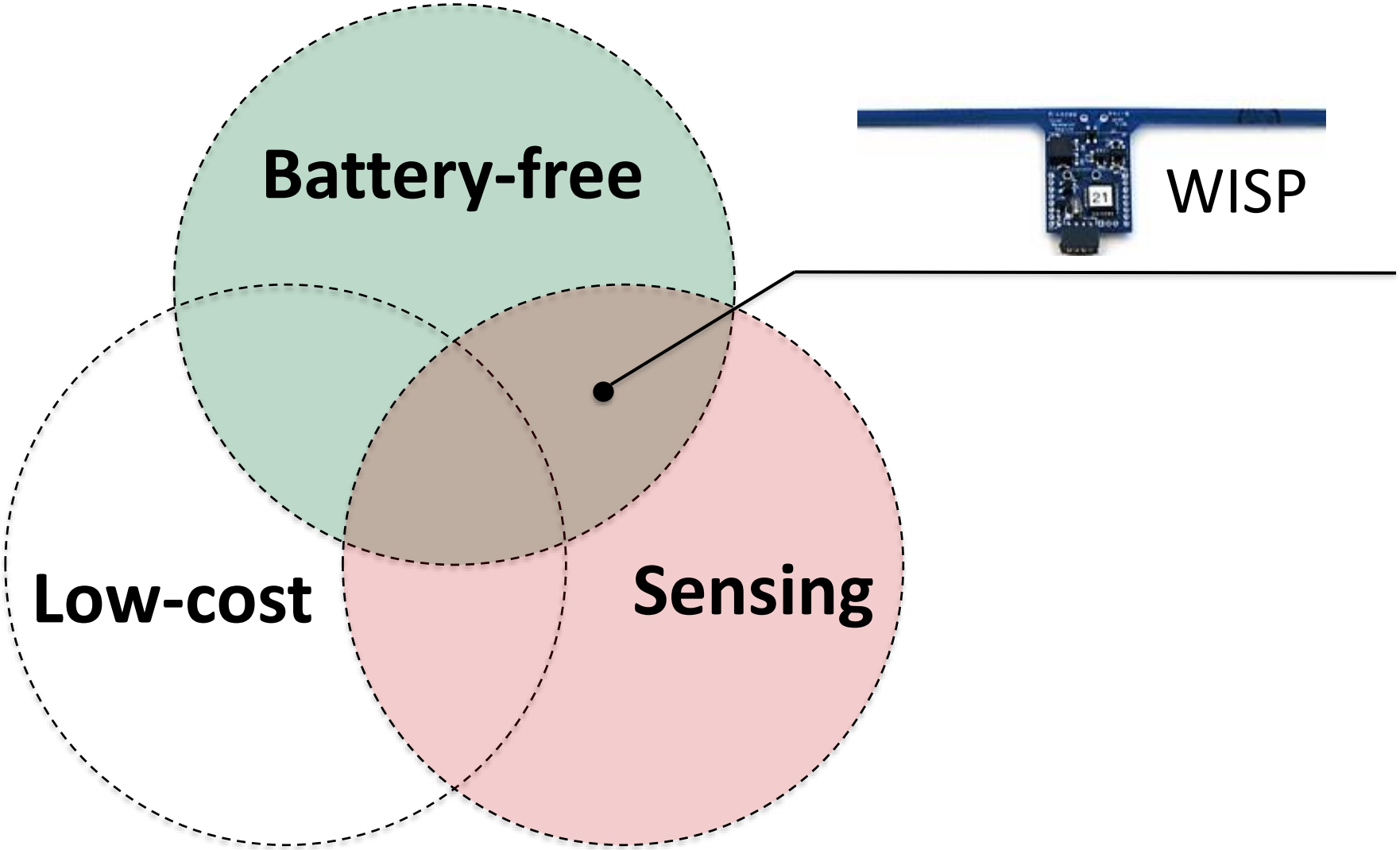
Ju Wang, Omid Abari and Srinivasan Keshav

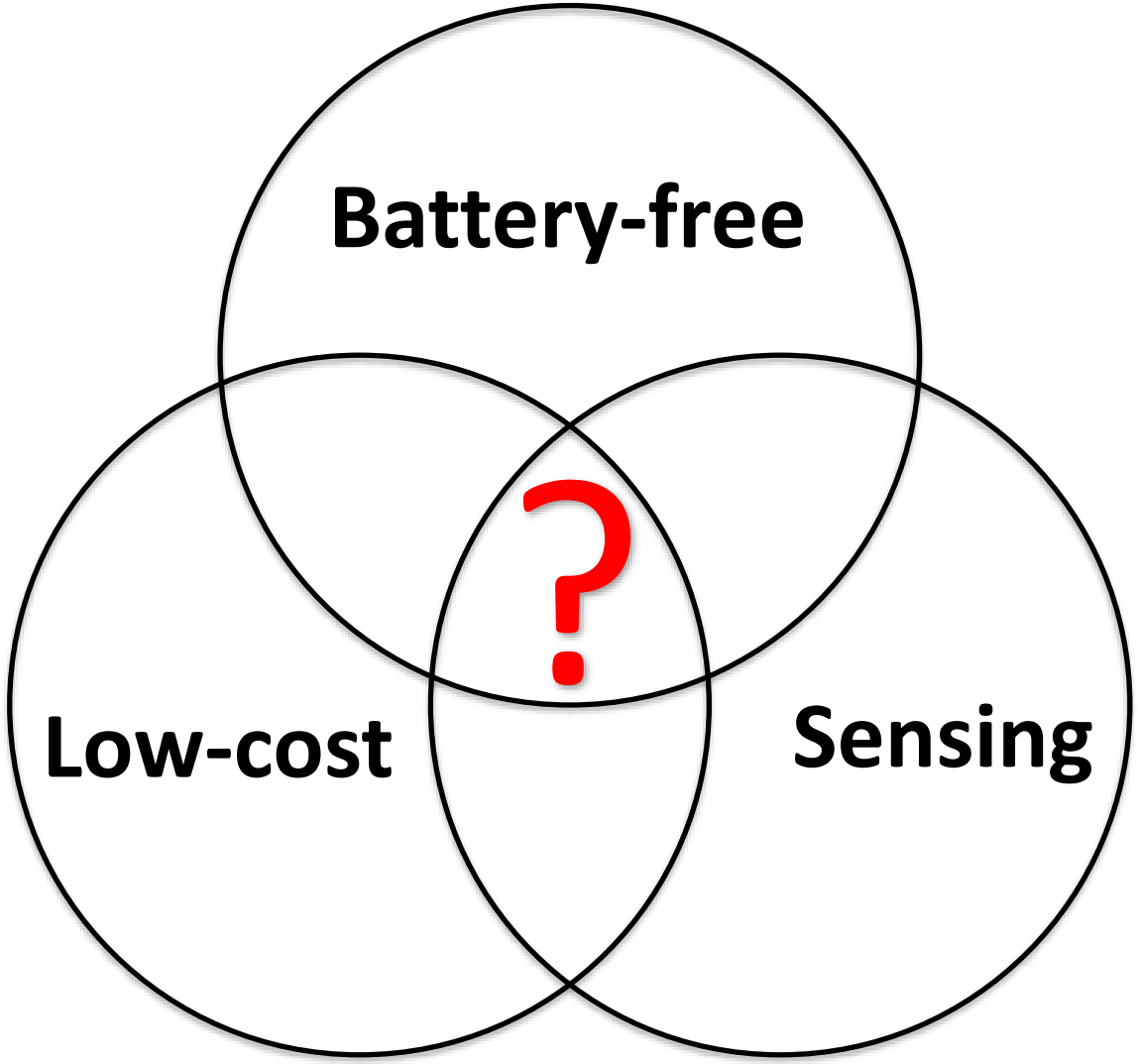
UNIVERSITY OF WATERLOO

ICONLAB.ca


Battery-free
Low-cost
Sensing

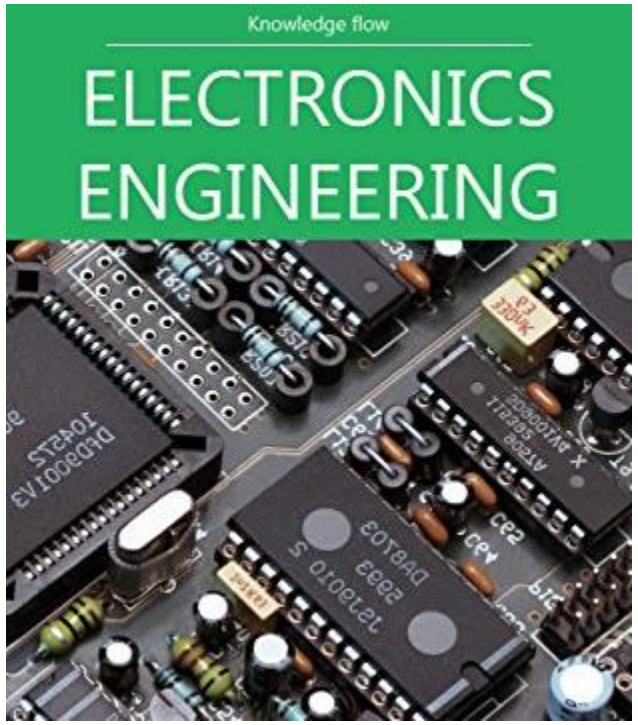

RFID
Battery-free
Low-cost
Sensing


Battery-free
Low-cost
Sensing
WISP

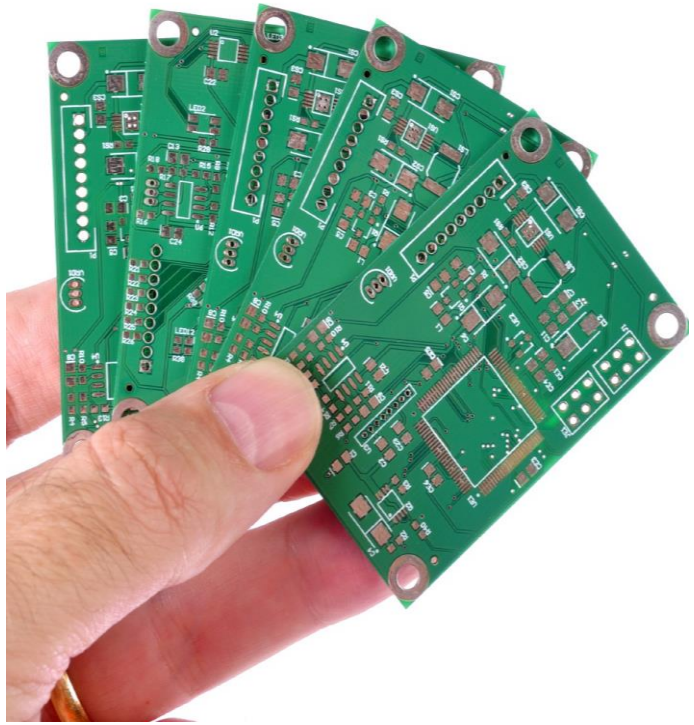

Battery-free
?
Low-cost
Sensing

Can we build low-cost, battery-free sensors?

Electronic knowledge



PCB design



Fabrication

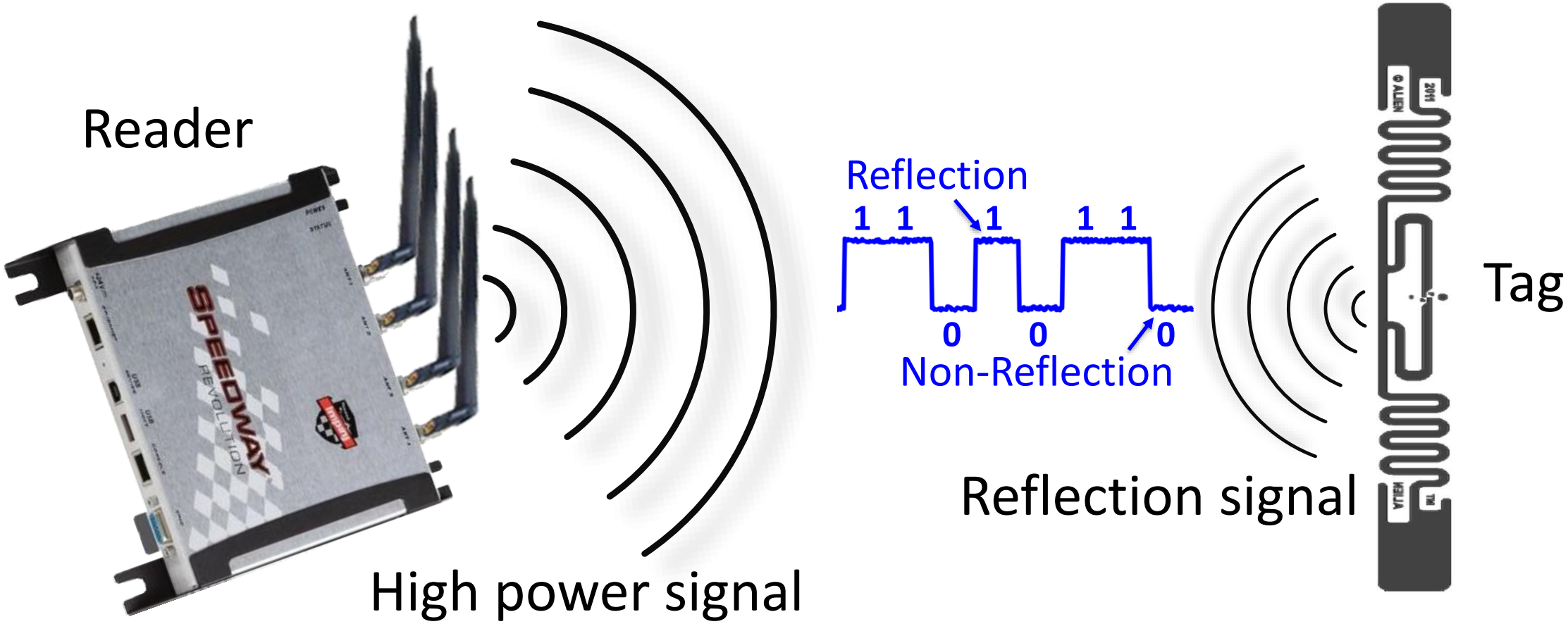
The process is costly & time consuming!

In this talk:

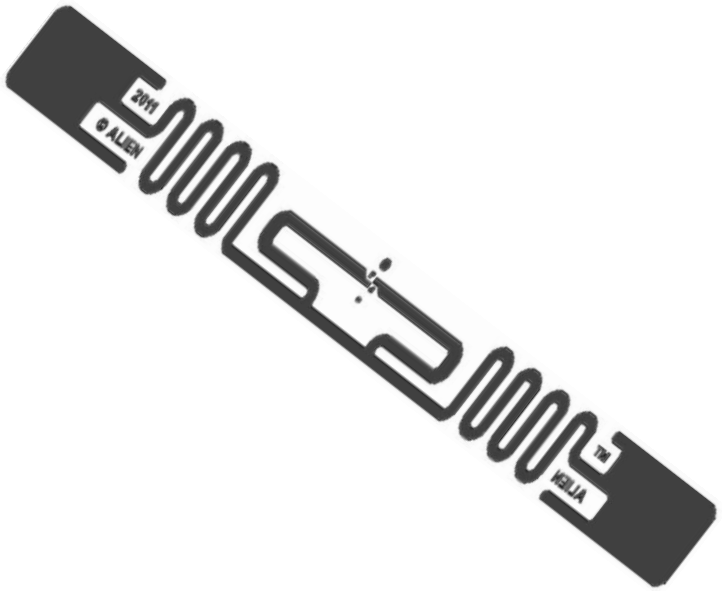
I will show how even a high school student can build low-cost, battery-free sensors by *hacking* RFID tags

What are RFIDs?

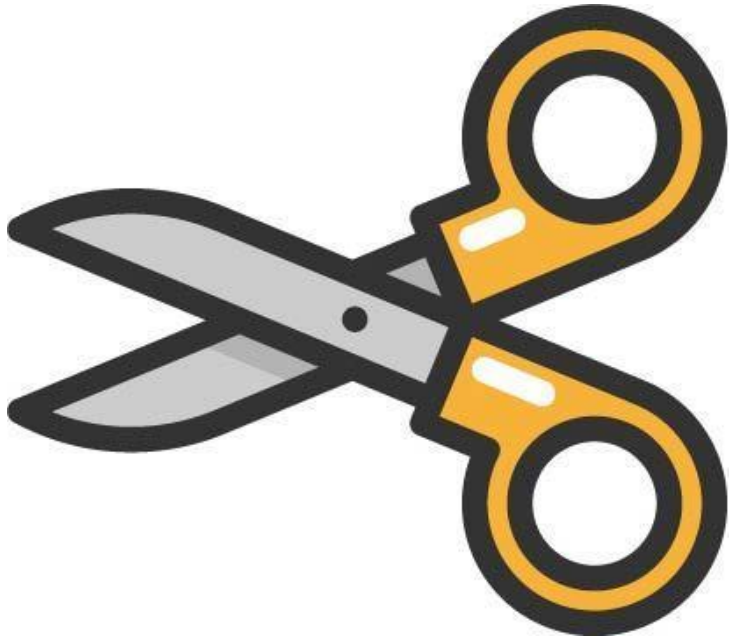
Cheap (5 cents), battery-free RF reflector with unique ID.



Converting RFIDs to the Light Sensor



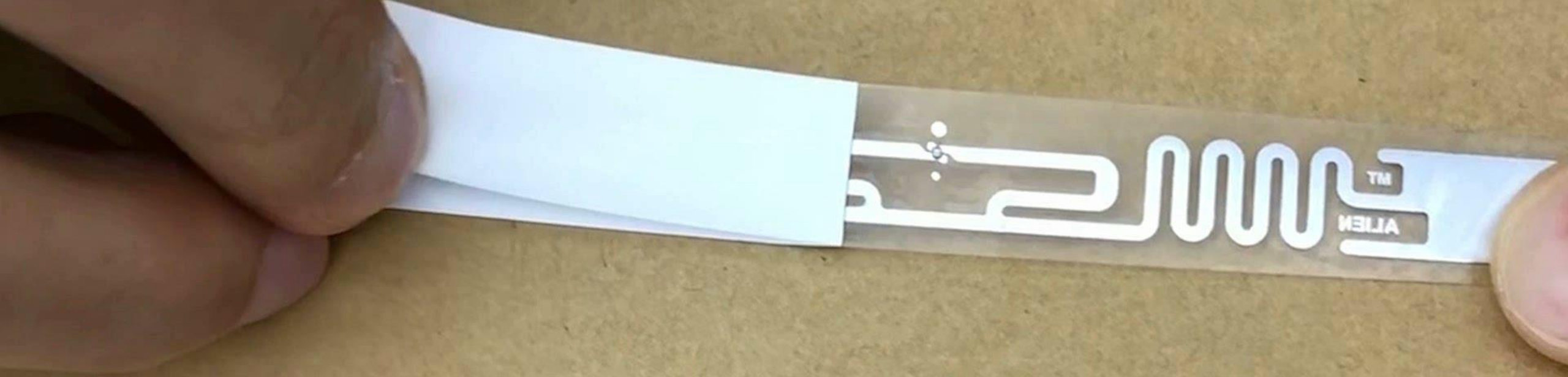
RFID Tag



Scissor

Photoresistor

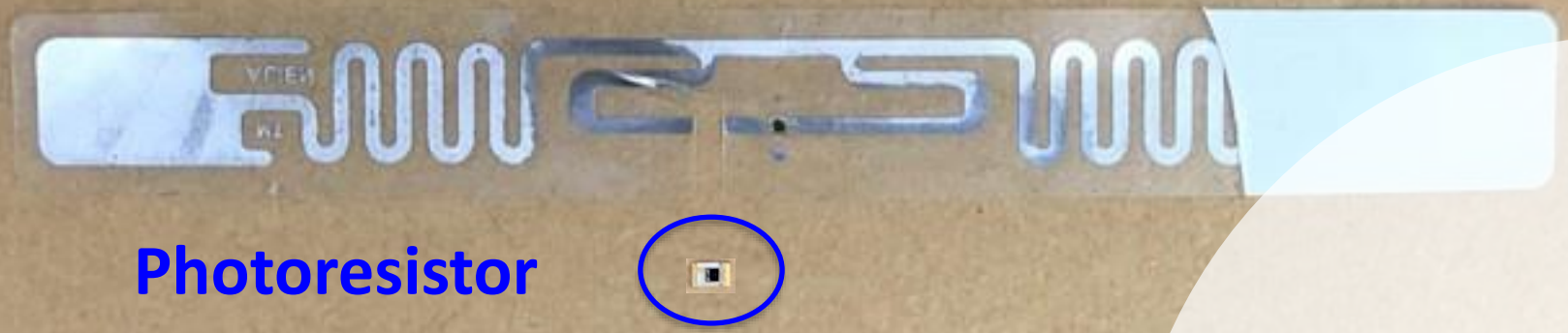
Step 1: Removing plastic cover



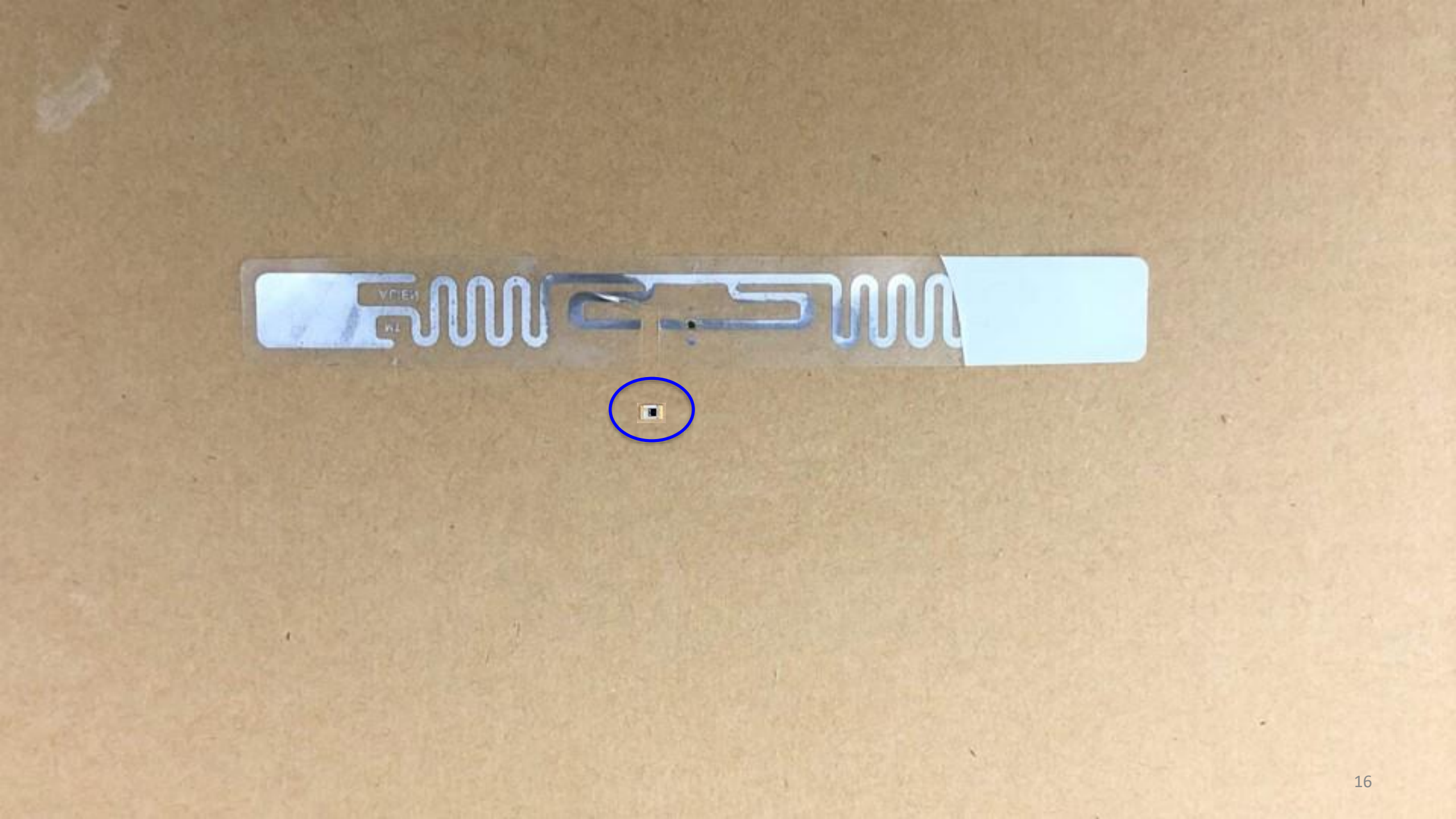
Plastic cover is removed

Step 2: Cutting the antenna


TM



Step 3: Placing a sensor

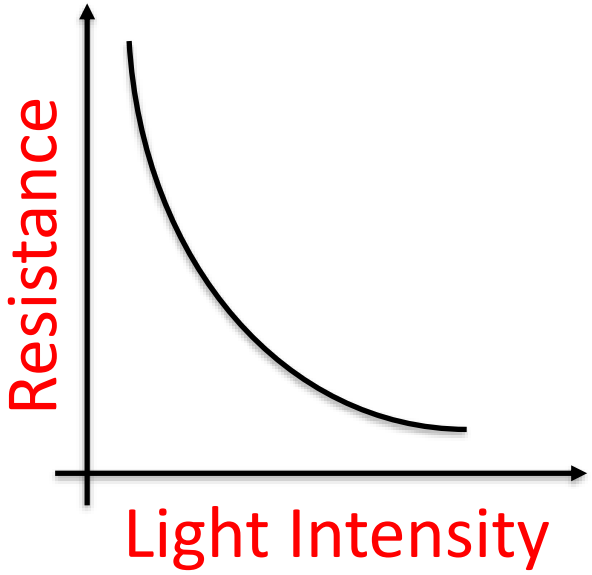


Battery-Free & Low-Cost, Light Sensor

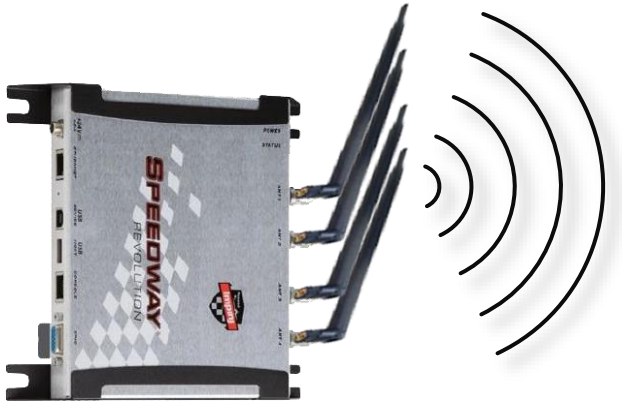
Converting RFIDs to the Light Sensor

Photoresistor

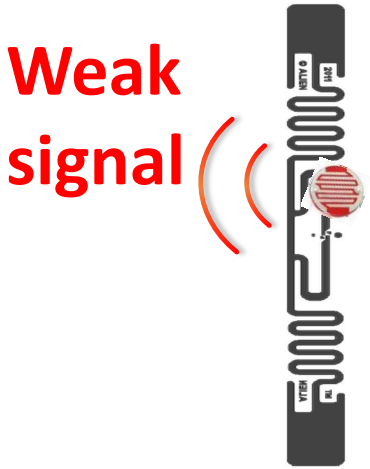
Modified Tag

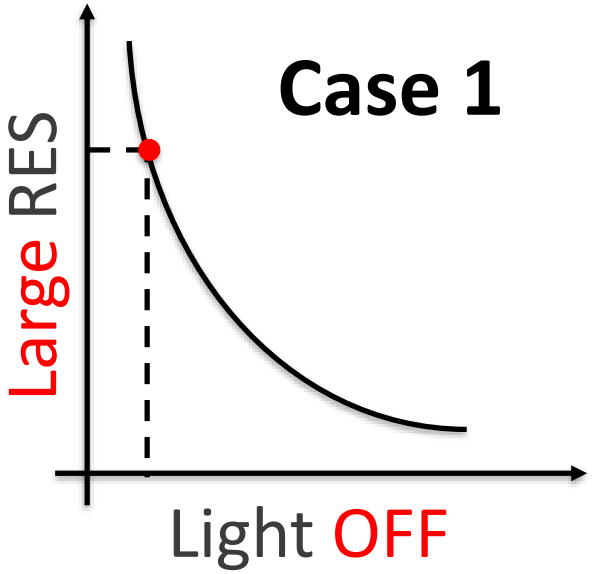


Converting RFIDs to the Light Sensor

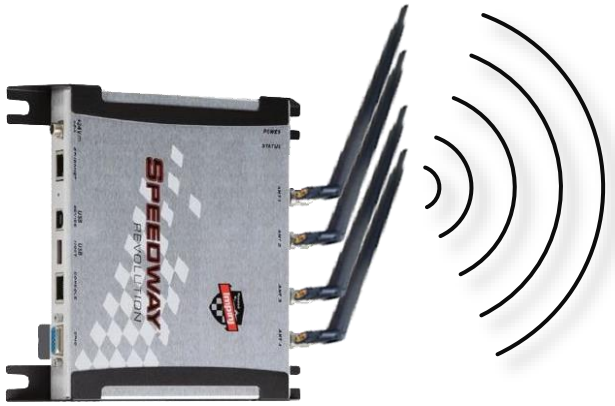


Reader



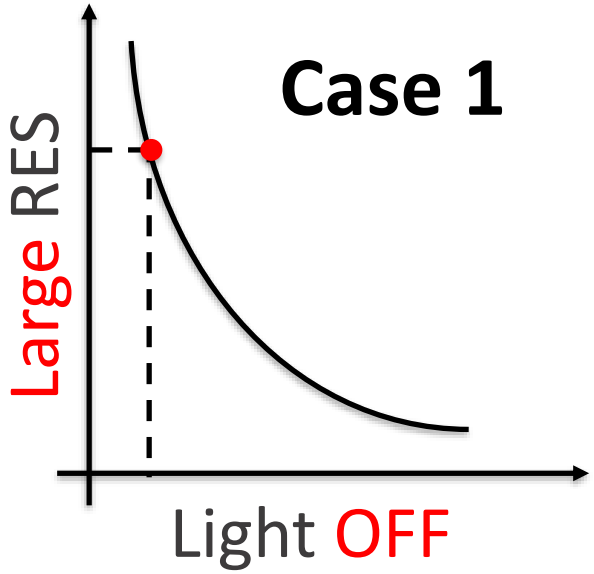


Converting RFIDs to the Light Sensor



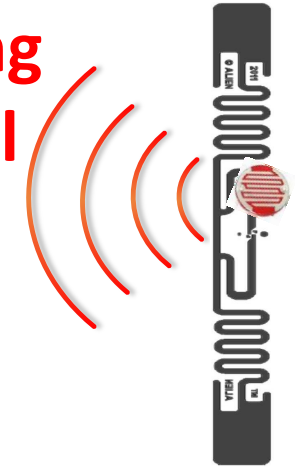
Reader

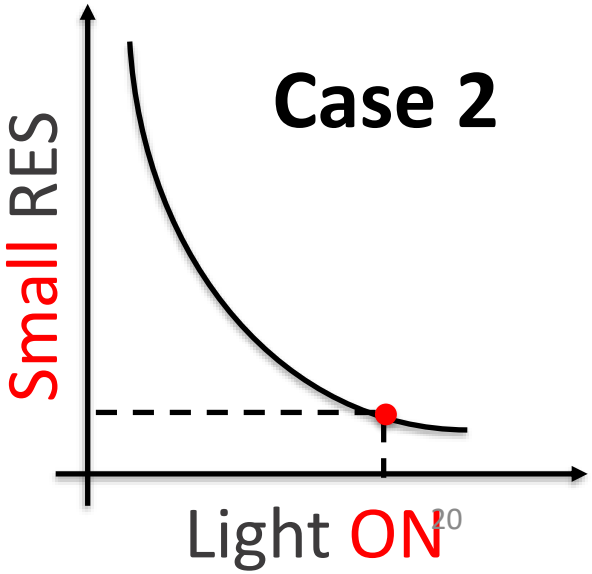
Weak signal



Reader

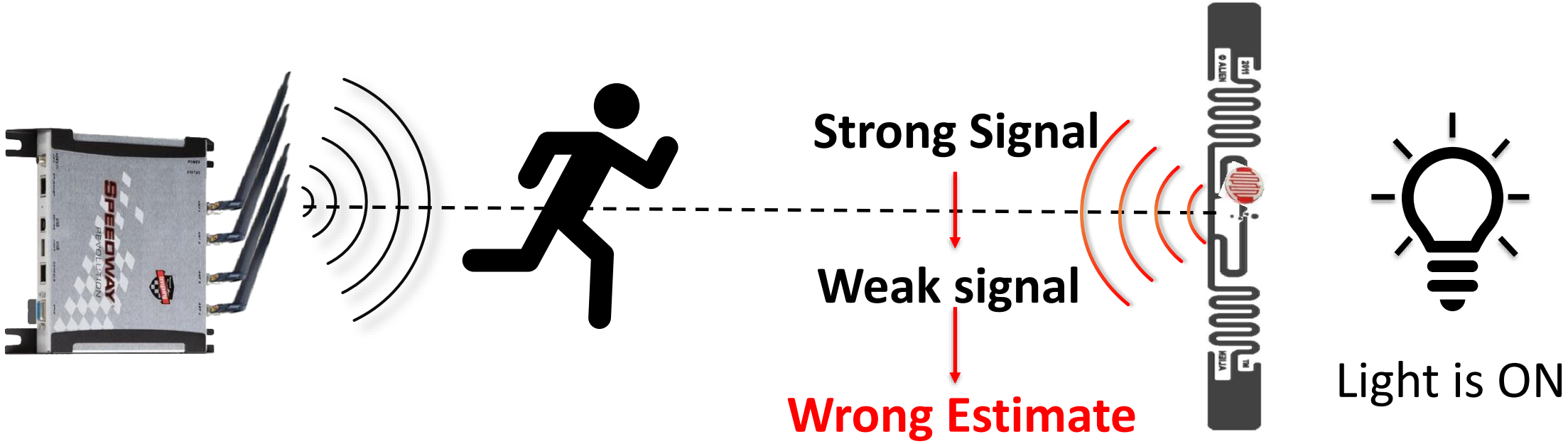
Strong signal



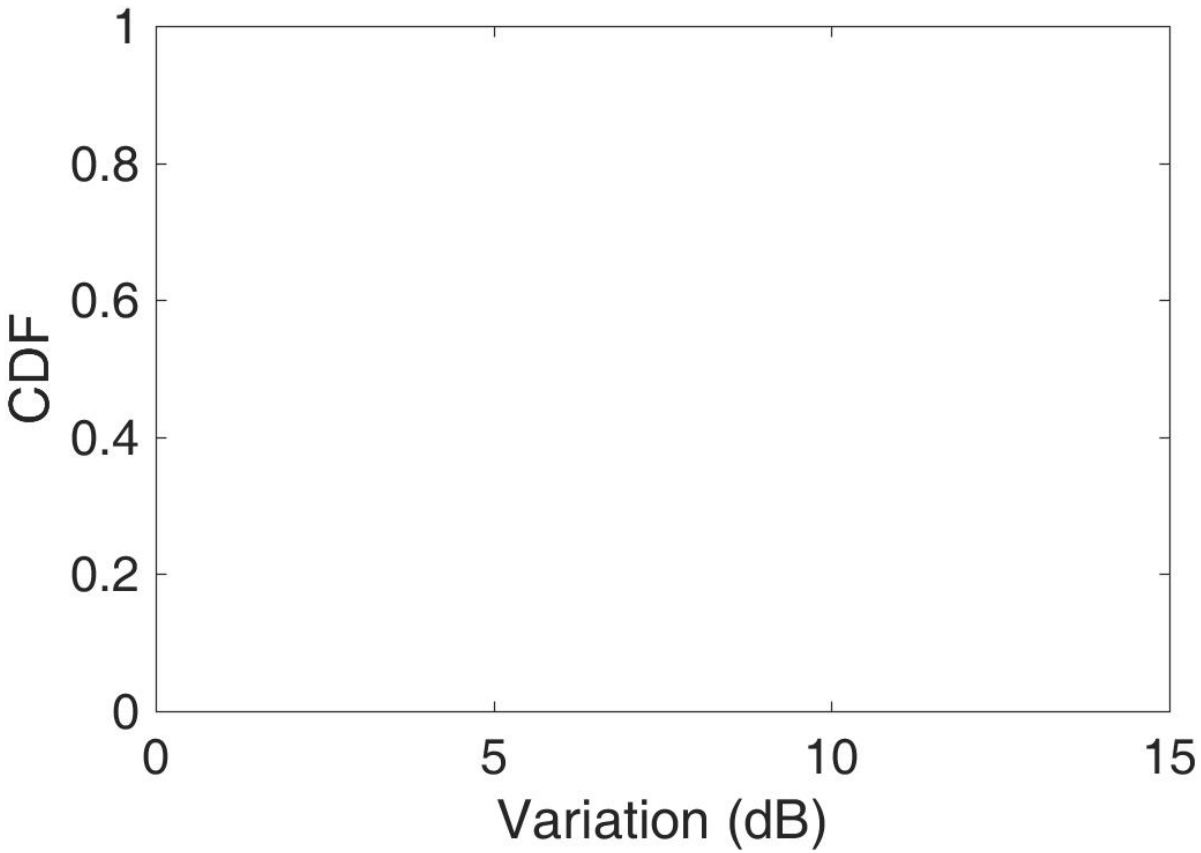


Challenge

Challenge

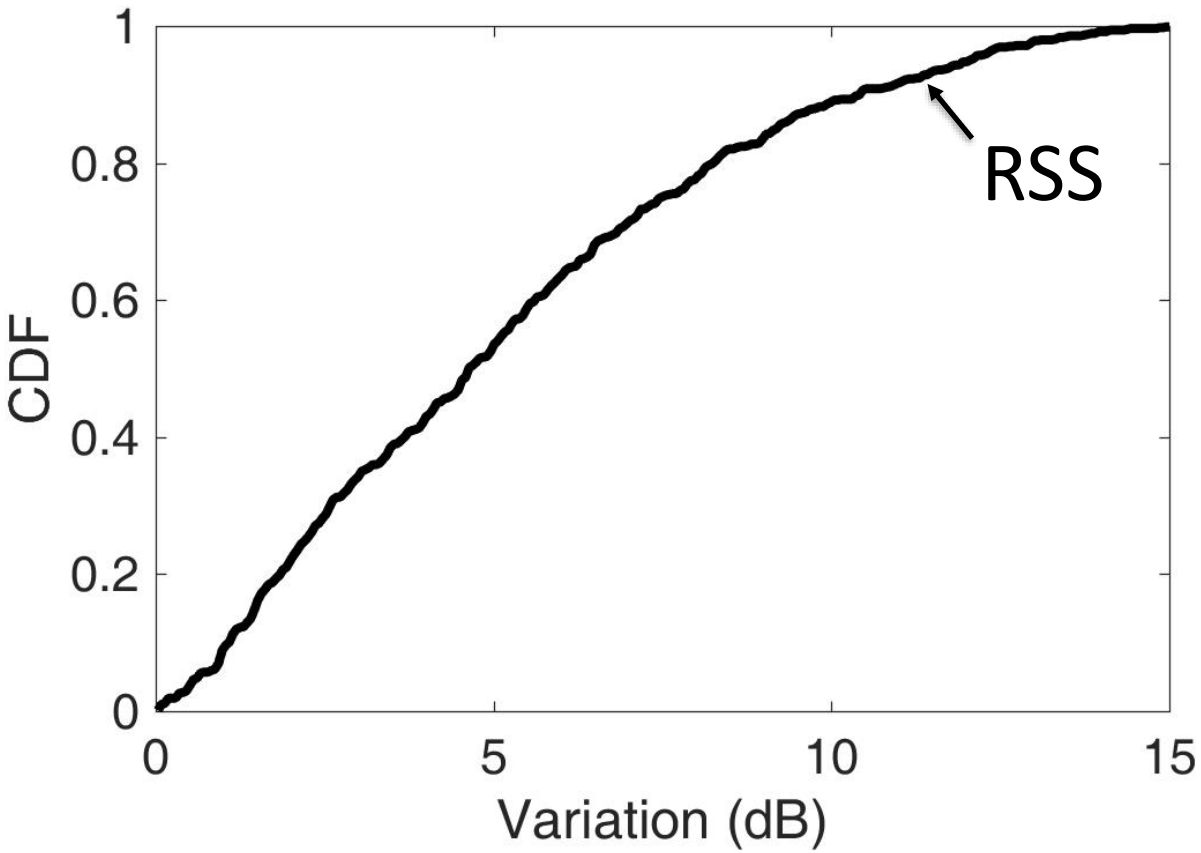


Challenge



Received signal strength (RSS) in a dynamic environment & fixed light intensity

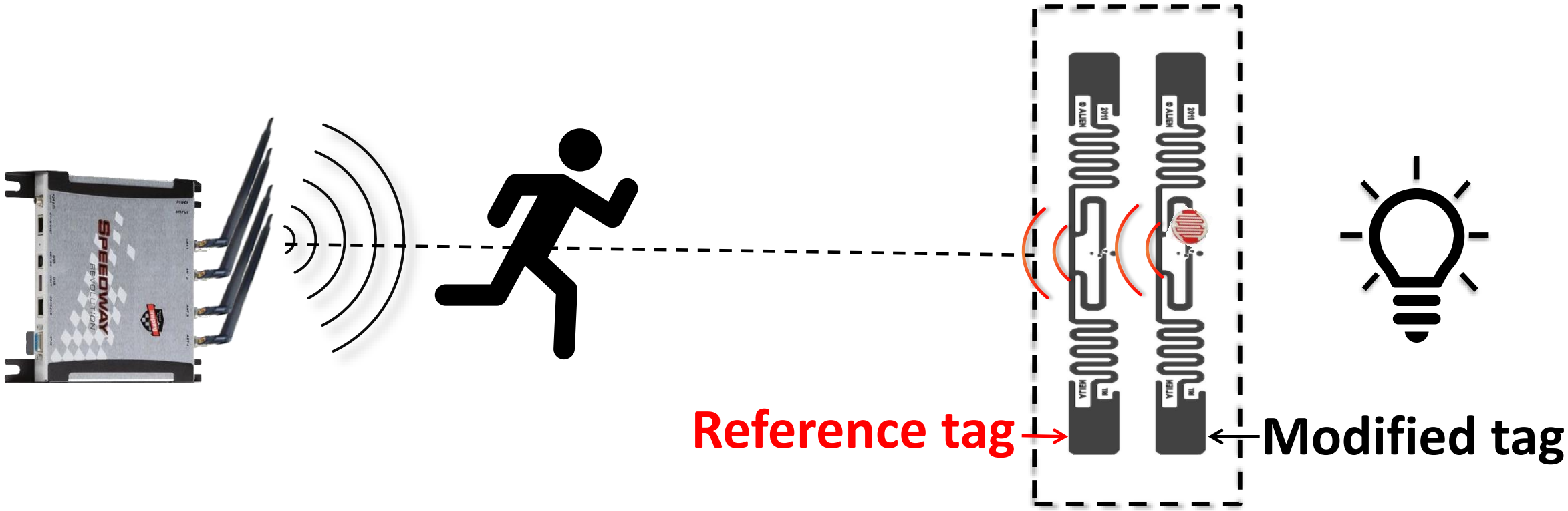
Challenge



Received signal strength (RSS) changes by both Light and Environment

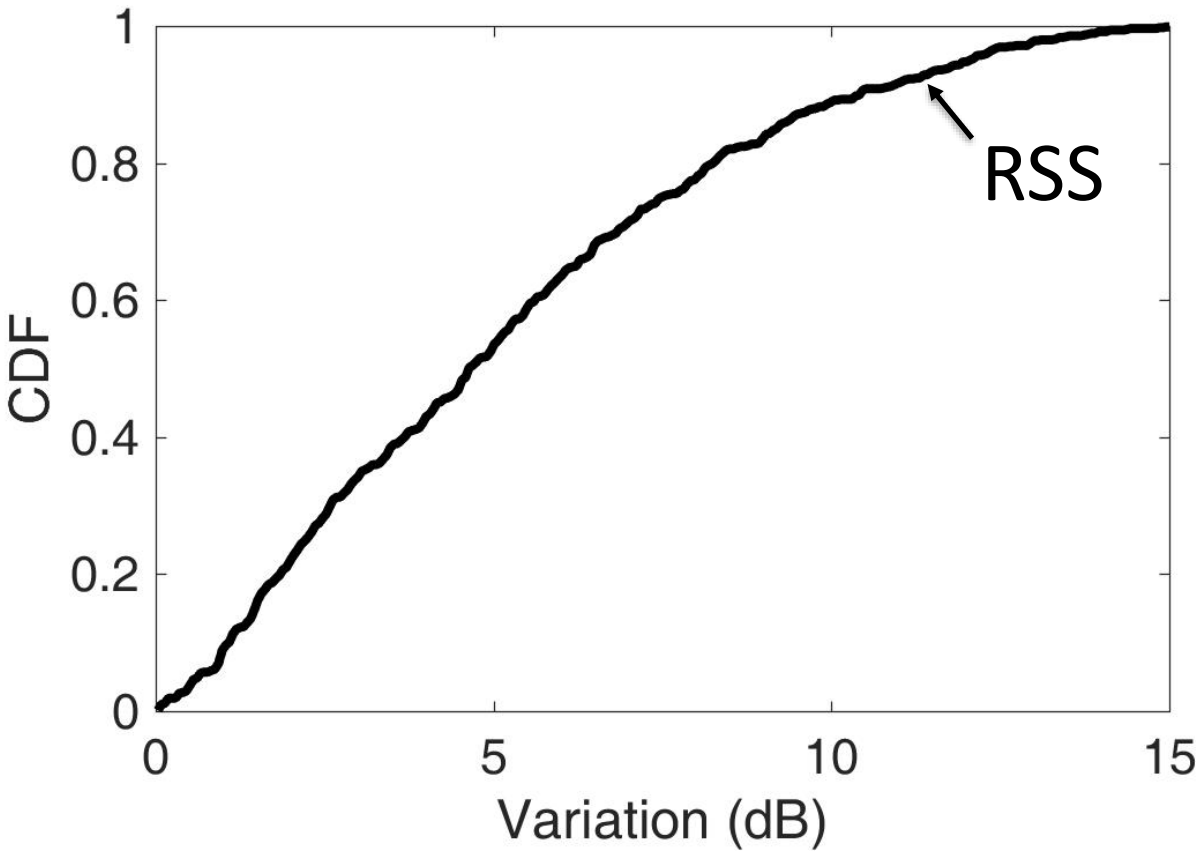
Solution: Differential Sensing

Solution: Differential Sensing



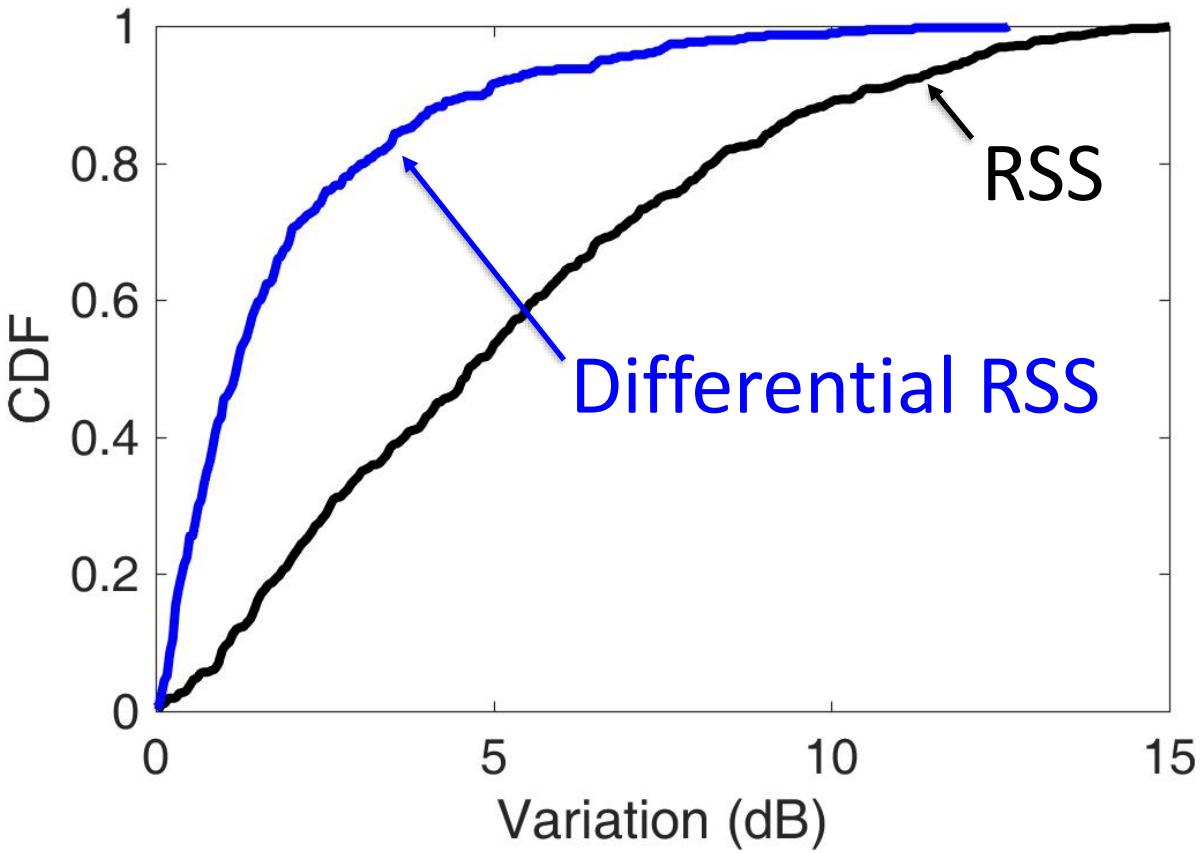
- **Reference tag**: RSS1 ∝ Environment
- **Modified tag**: RSS2 ∝ Light + Environment
- **Differential: (RSS2 – RSS1) ∝ Light**

Does Differential Sensing Help?



RSS in a dynamic environment & fixed light intensity

Does Differential Sensing Help?



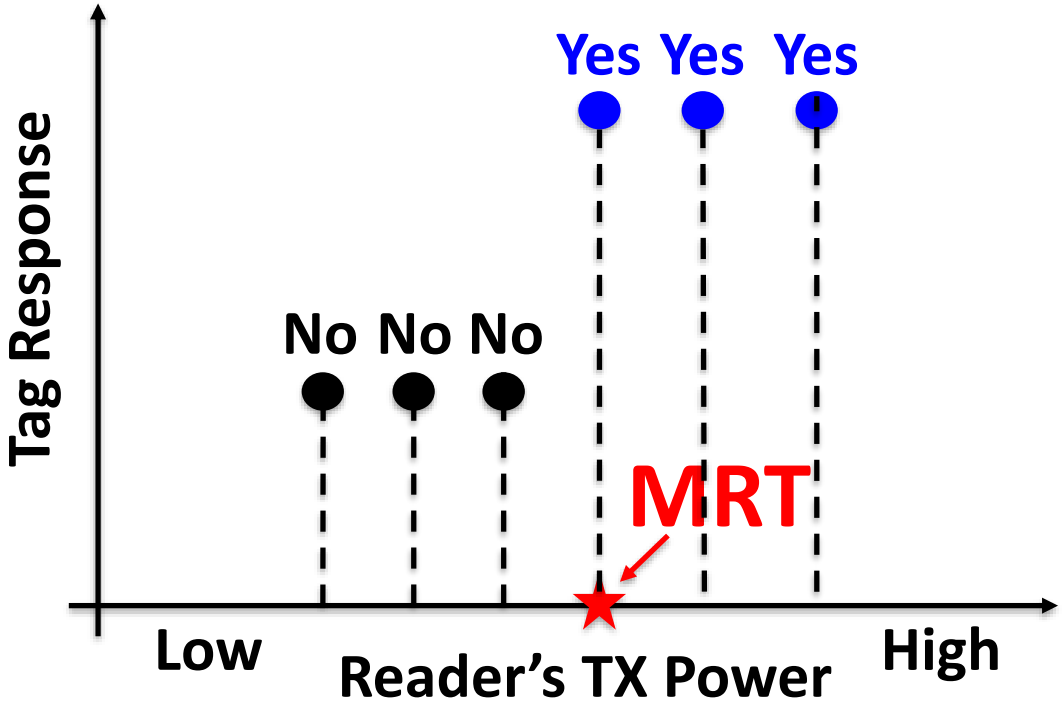
Even with differential sensing, the differential RSS is still unstable.

Our Solution: Minimum Response Threshold (MRT)

High power signal actives tags.

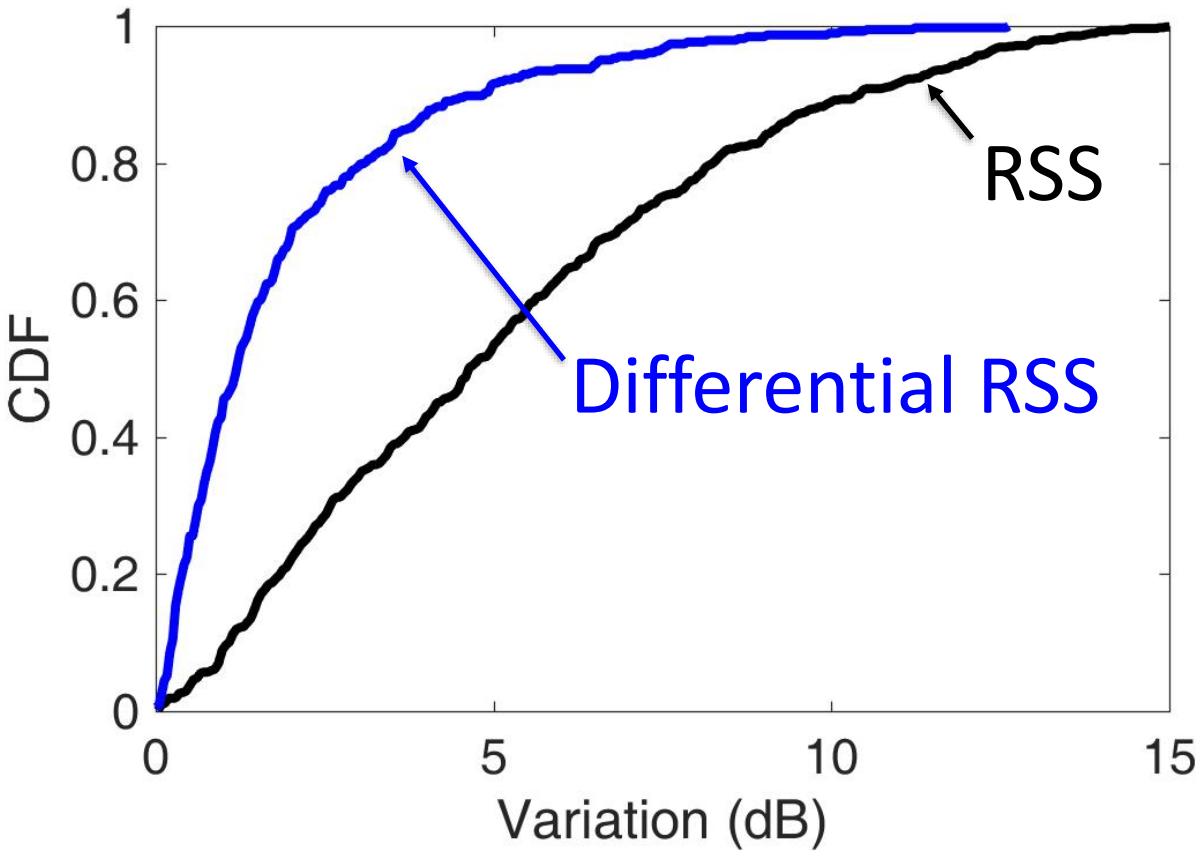
Our Solution: Minimum Response Threshold (MRT)

High power signal actives tags.



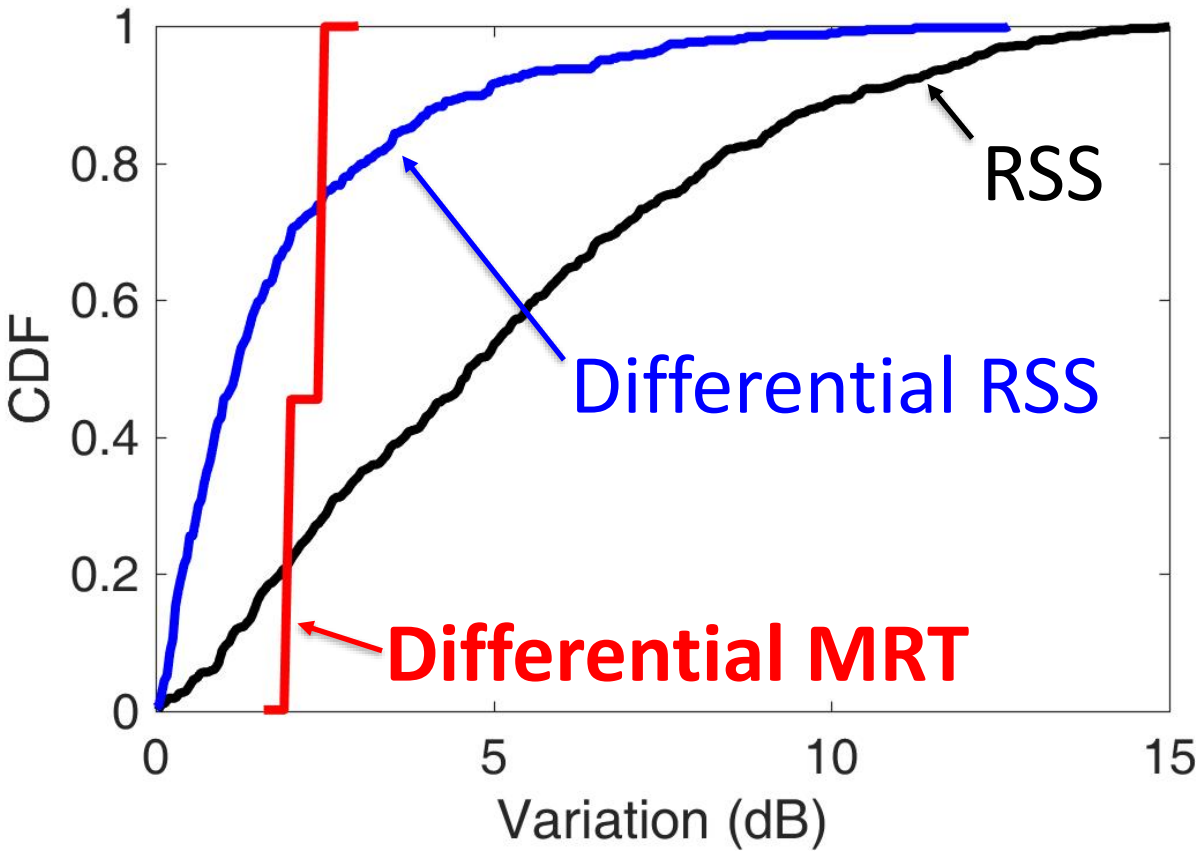
MRT: the required minimum TX power to activate a tag.

Advantage of Differential MRT



Comparison of RSS, Differential RSS and Differential MRT

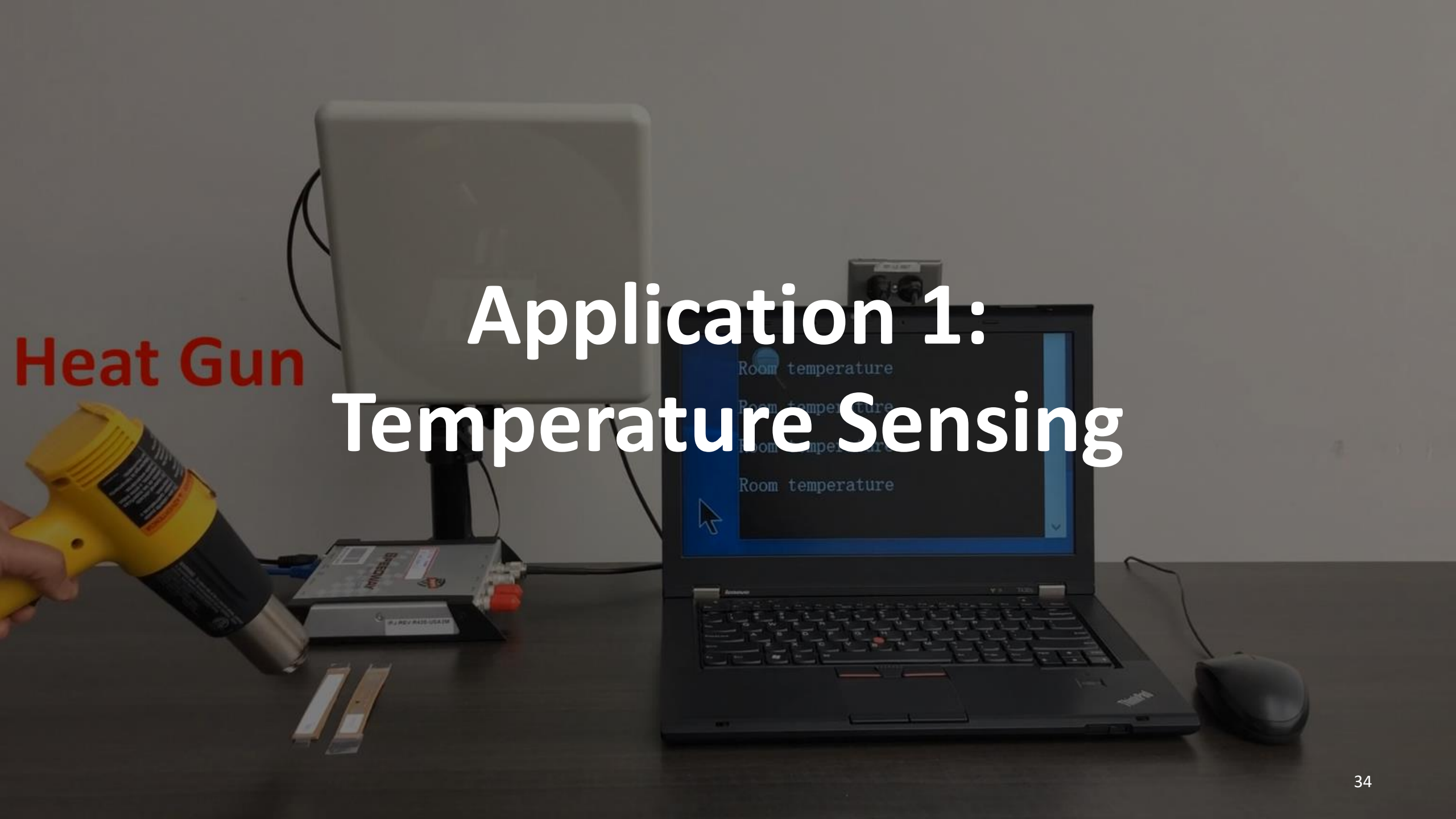
Advantage of Differential MRT

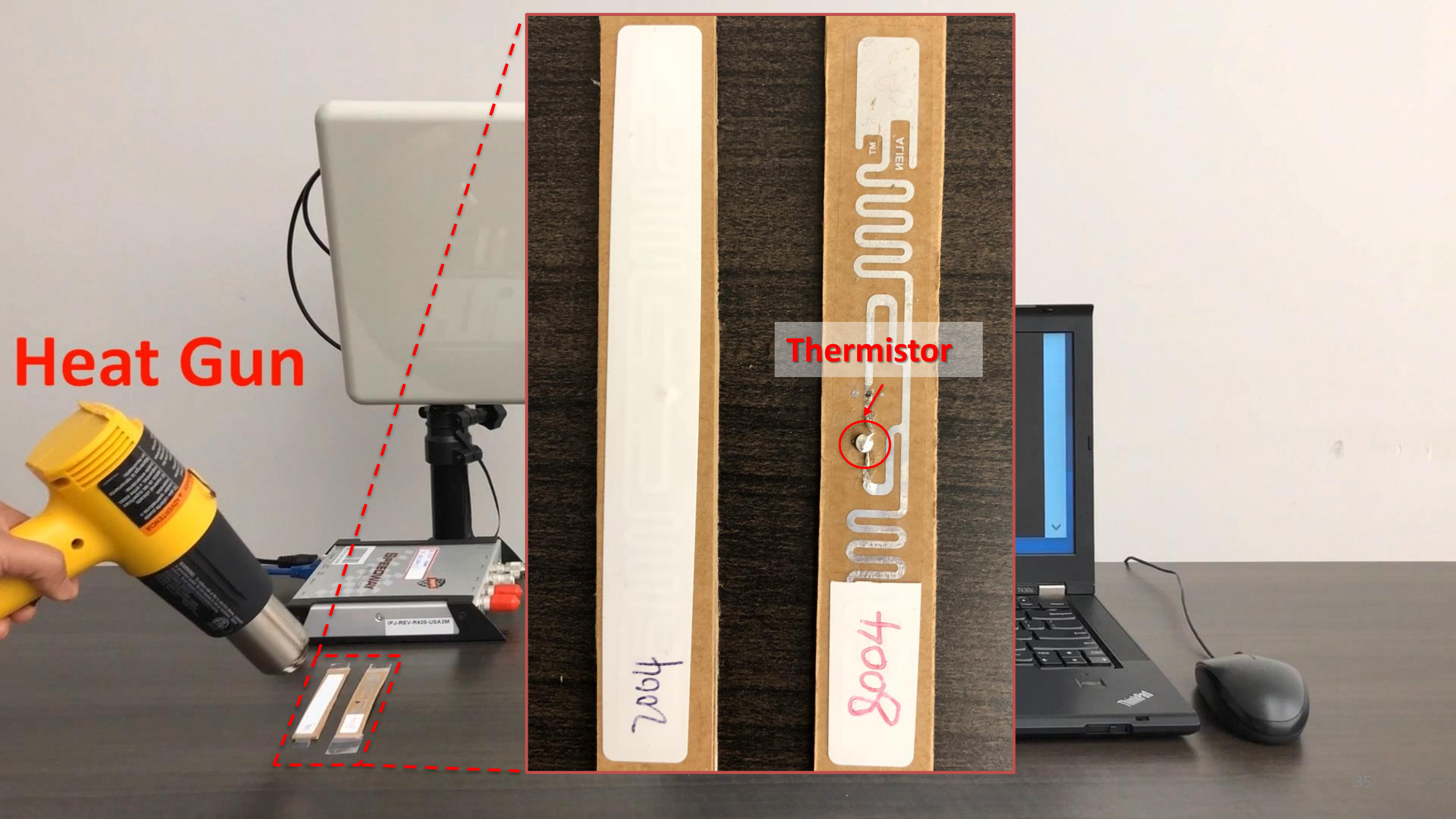


Differential MRT is very stable, with a 90% variations < 2.5 dB.

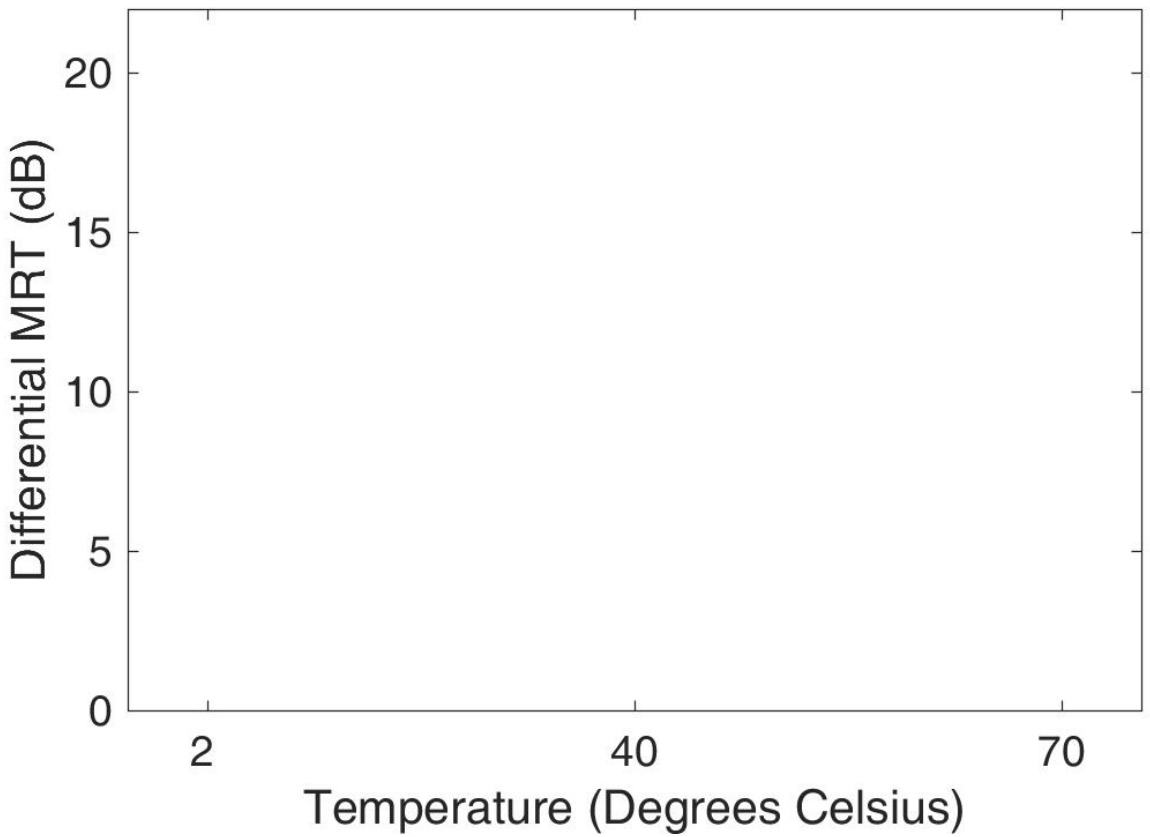
Applications & Results

Application 1: Temperature Sensing

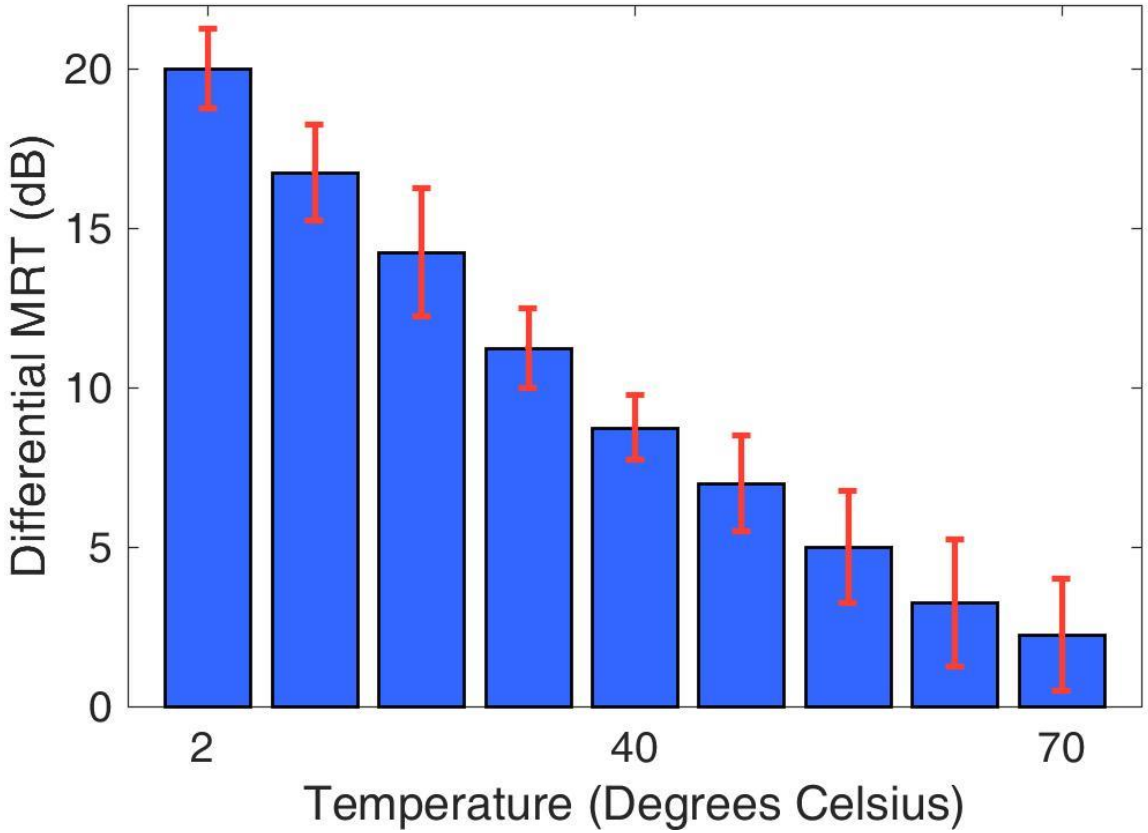



Heat Gun
Thermistor
ALIEN
8004
4002

Temperature Sensing Evaluation

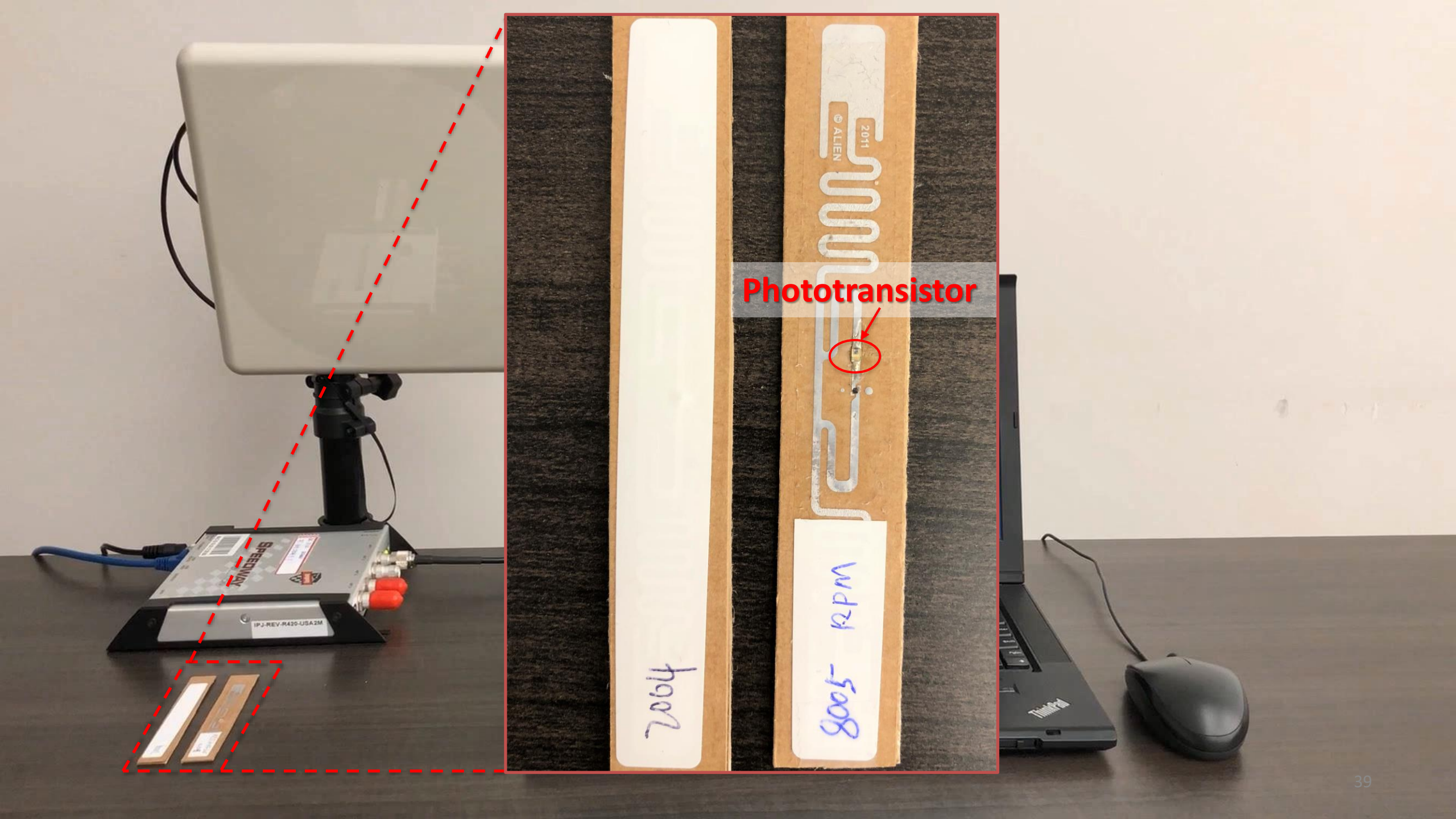


Temperature Sensing Evaluation

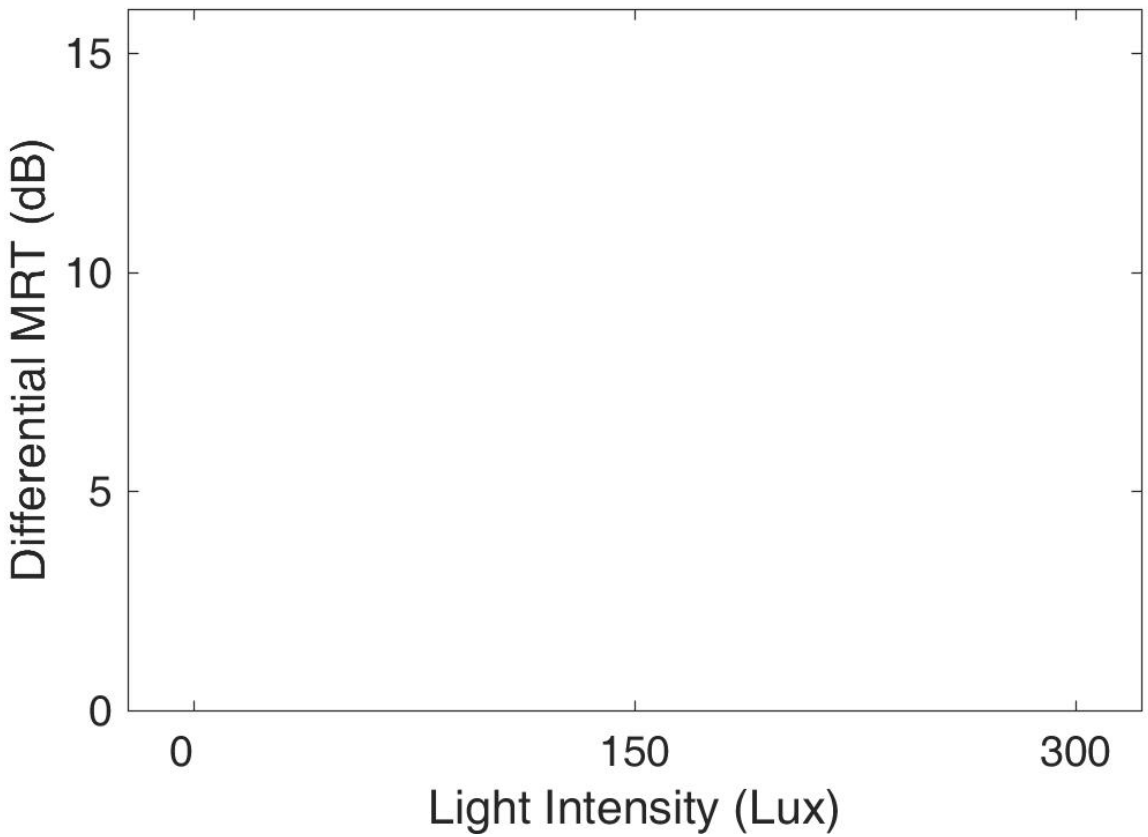


Our sensor works over a wide range of temperature

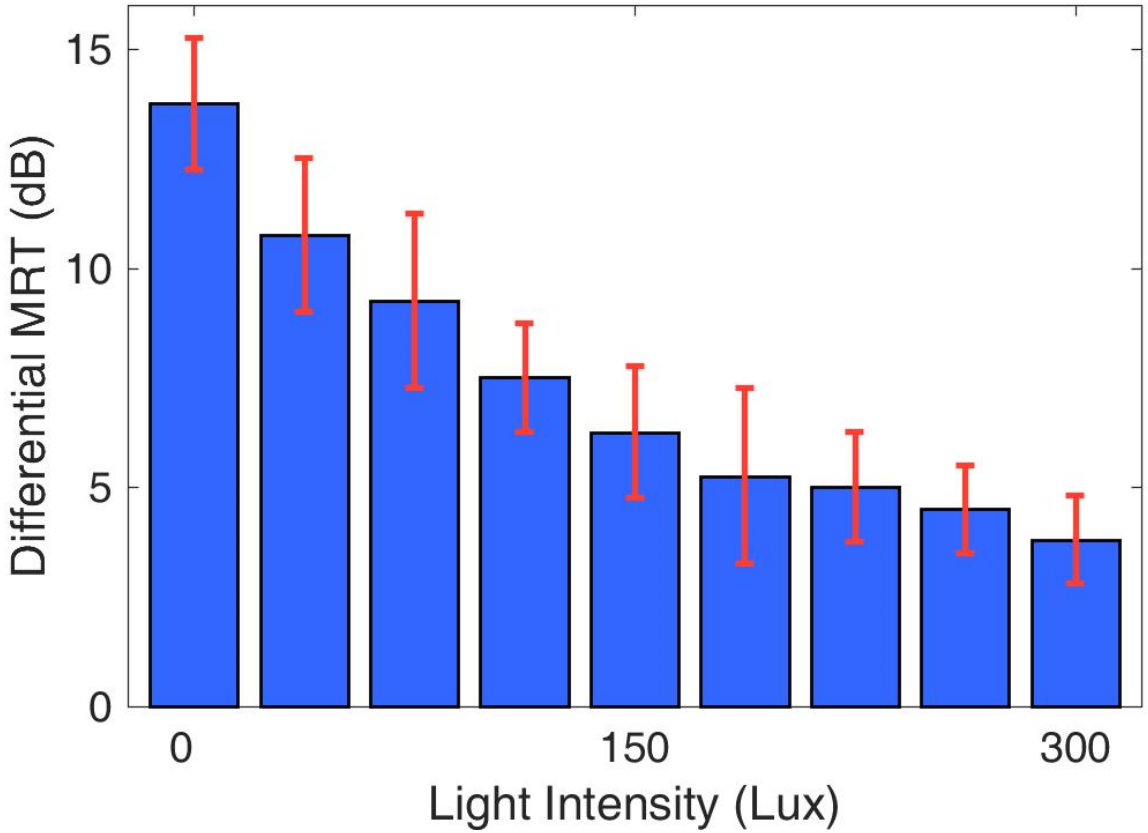
Application 2: Light Sensing


Phototransistor
ALIEN
2011
SPEEDWAY
IPJ-REV-R420-USA2M
ThinkPad

Light Sensing Evaluation

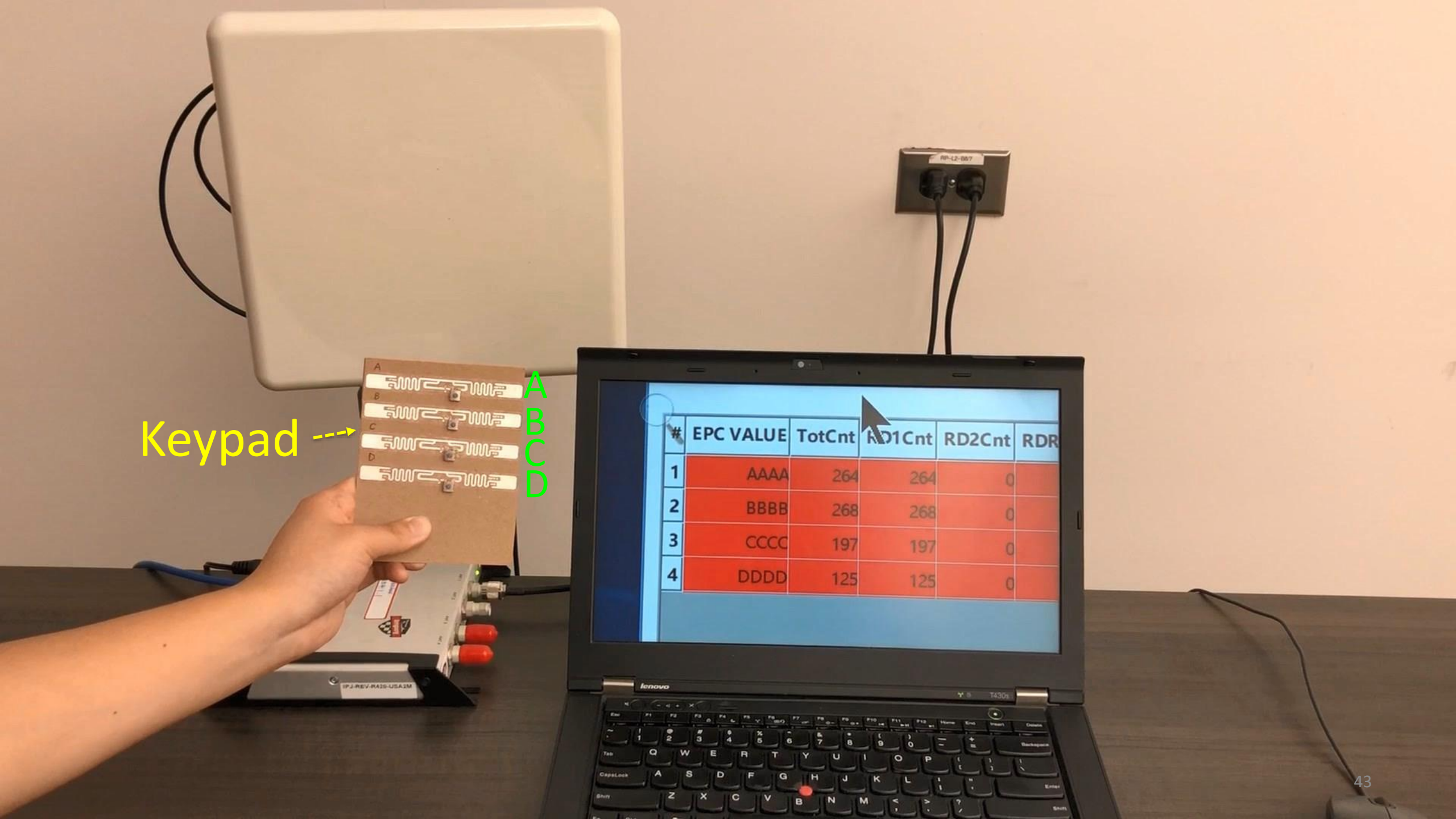


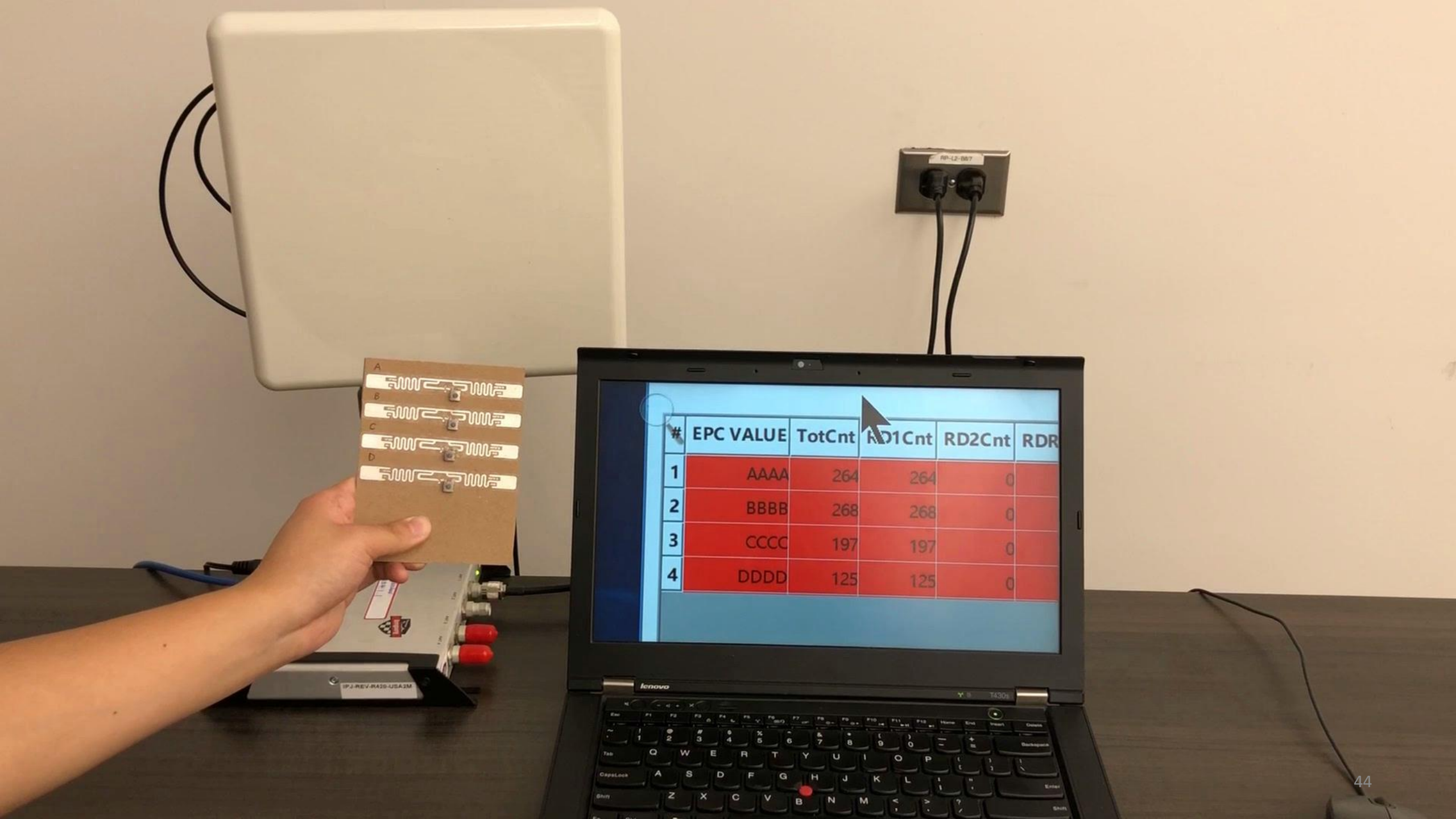
Light Sensing Evaluation



We can estimate light intensity using RFID tags

Application 3: battery-free Keypad


Keypad
A
B
C
D
EPC VALUE TotCnt RD1Cnt RD2Cnt RDR
1 AAAA 264 264 0
2 BBBB 268 268 0
3 CCCC 197 197 0
4 DDDD 125 125 0



#	EPC VALUE	TotCnt	RD1Cnt	RD2Cnt	RDR
1	AAAA	264	264	0	
2	BBBB	268	268	0	
3	CCCC	197	197	0	
4	DDDD	125	125	0	

Other Applications

Low-cost, battery-free:

- Humidity sensing
- Pressure sensing
- Keyboard
- …

Pressure sensor

Humidity sensor

Keyboard button

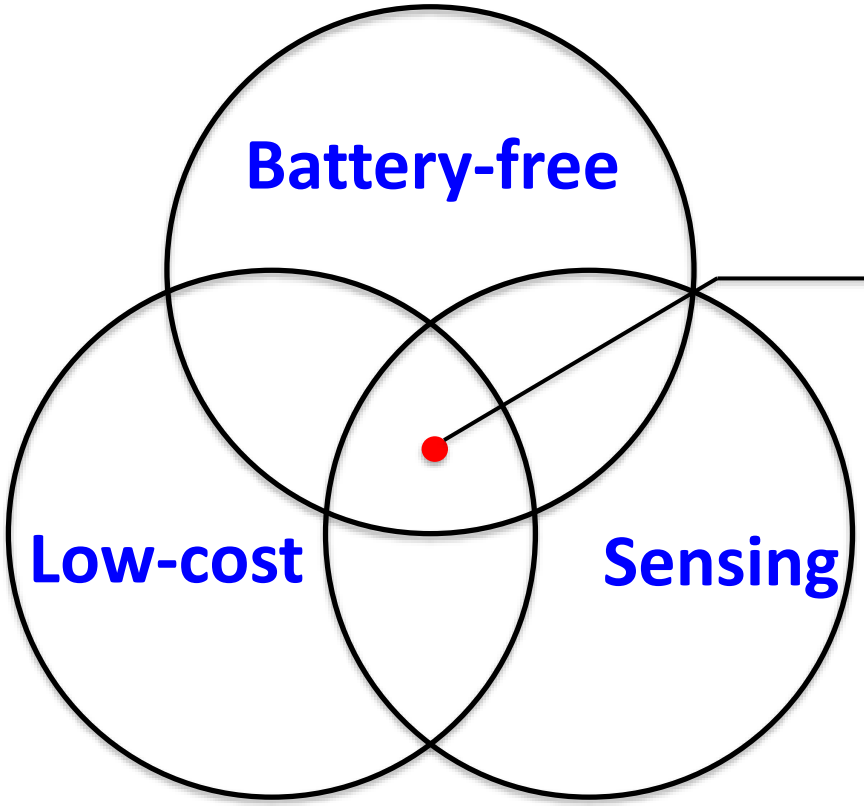
Limitations & Challenges

- **Improving the sensing range.**
  - Impedance matching between sensors and tag antenna.

- **Improving the sensing accuracy.**
  - Improving the resolution of Differential MRT.
  - Identifying `good' sensors that consistently detune tag's antenna gain.

- **Reducing the reader cost.**
  - Designing a low-cost RFID reader is still an open challenge.

Conclusion



Our approach:

Designing the low-cost, battery-free sensors by hacking cheap RFID tags.

Differential MRT:

A new sensing feature, which is robust to changes in the RF environment.