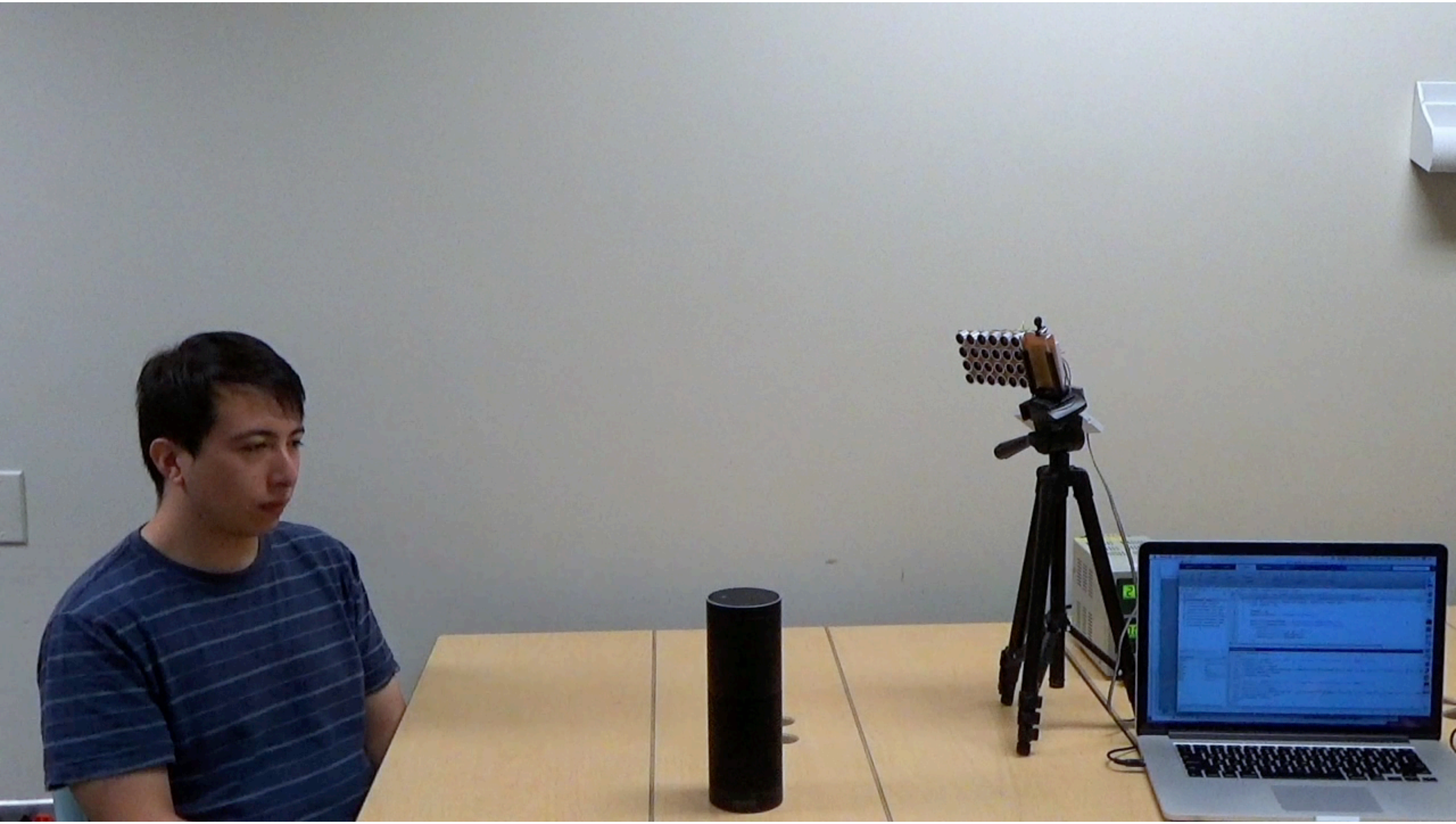
Physical Security Attacks

- Inertial (WALNUT)
- GPS Spoofing (Drone)
- Hacking Pacemakers
- Inaudible Voice Commands

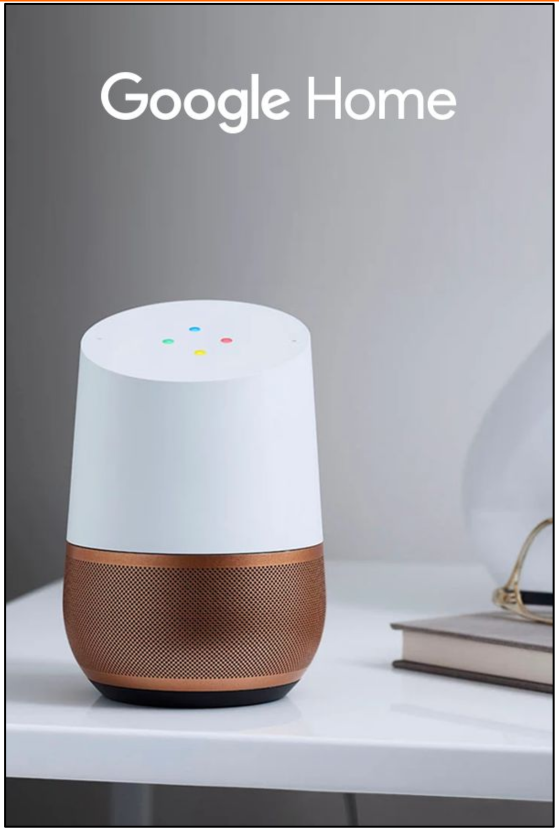
Mobile Security

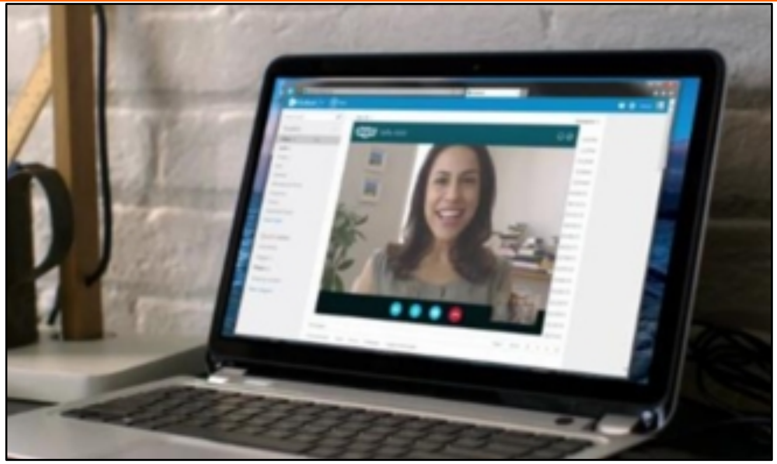
Inaudible Voice Commands

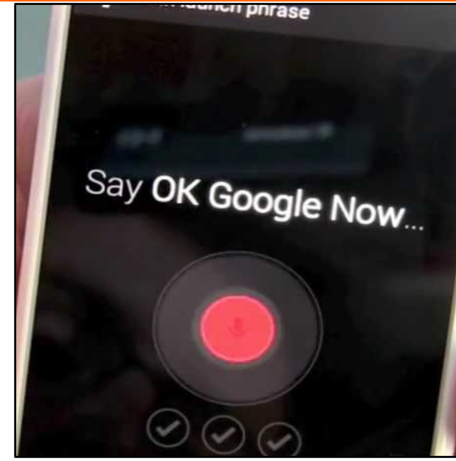


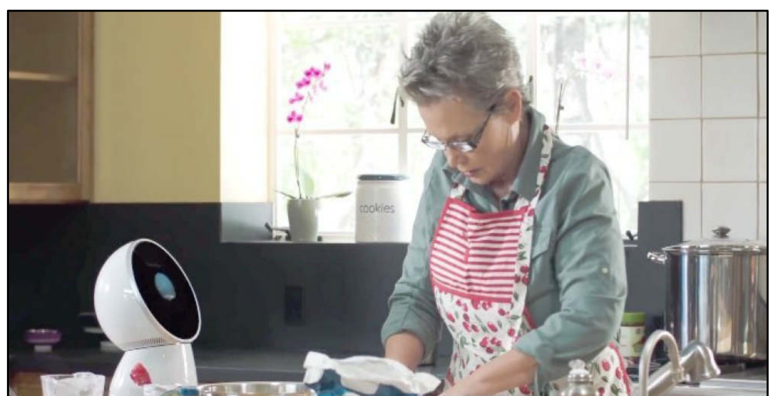
BackDoor: Making Microphones Hear Inaudible Sounds

Microphones are everywhere

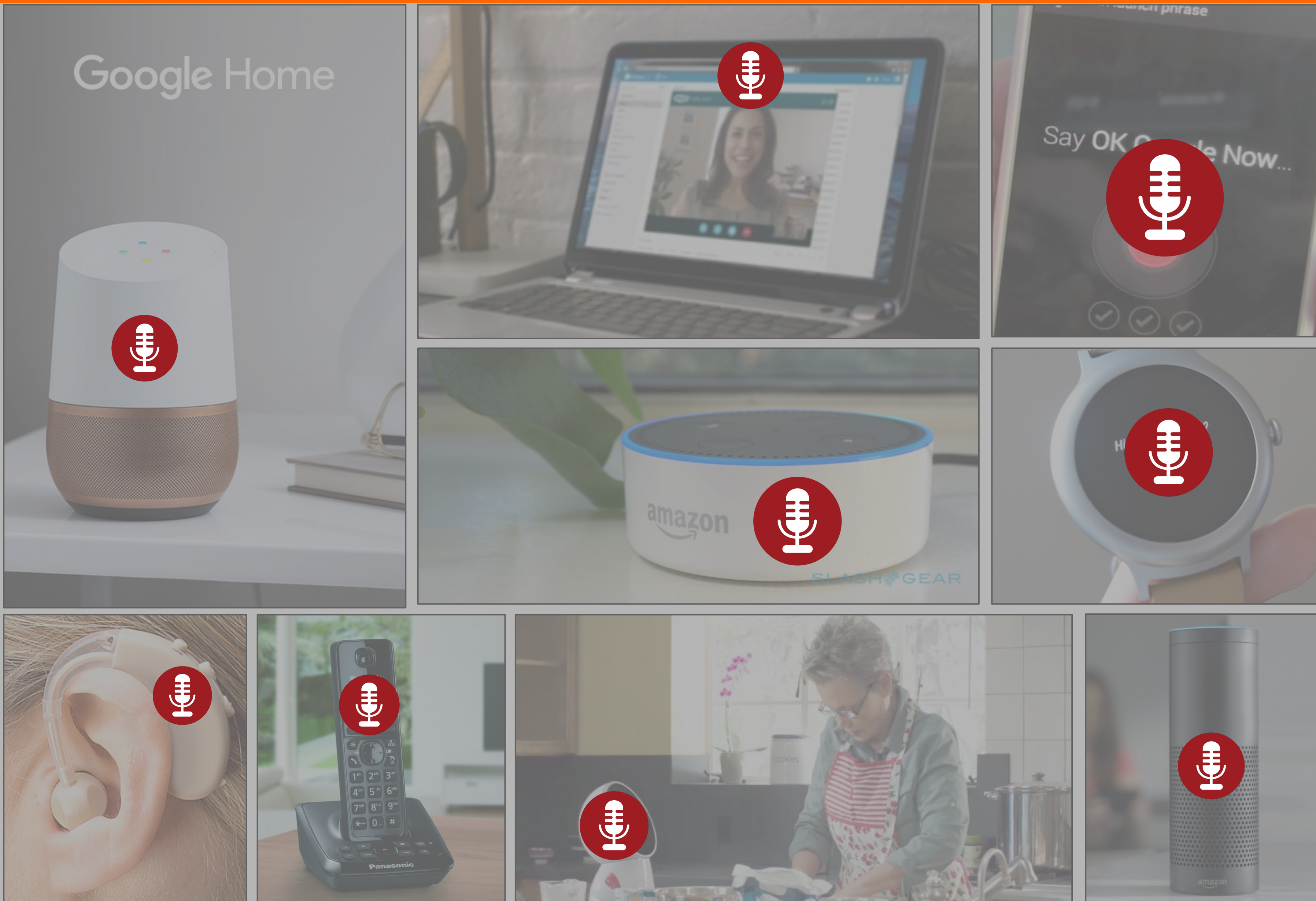




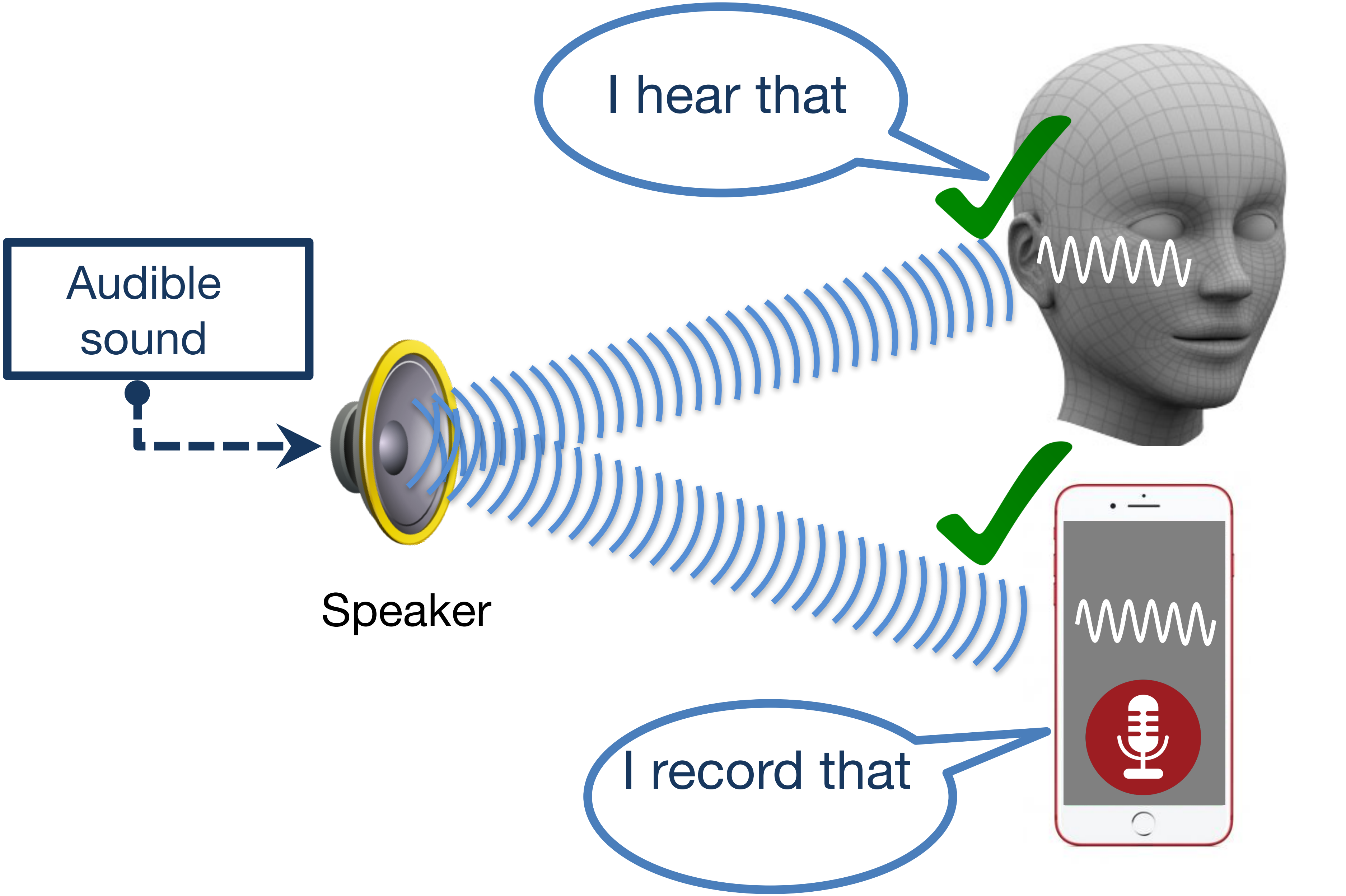




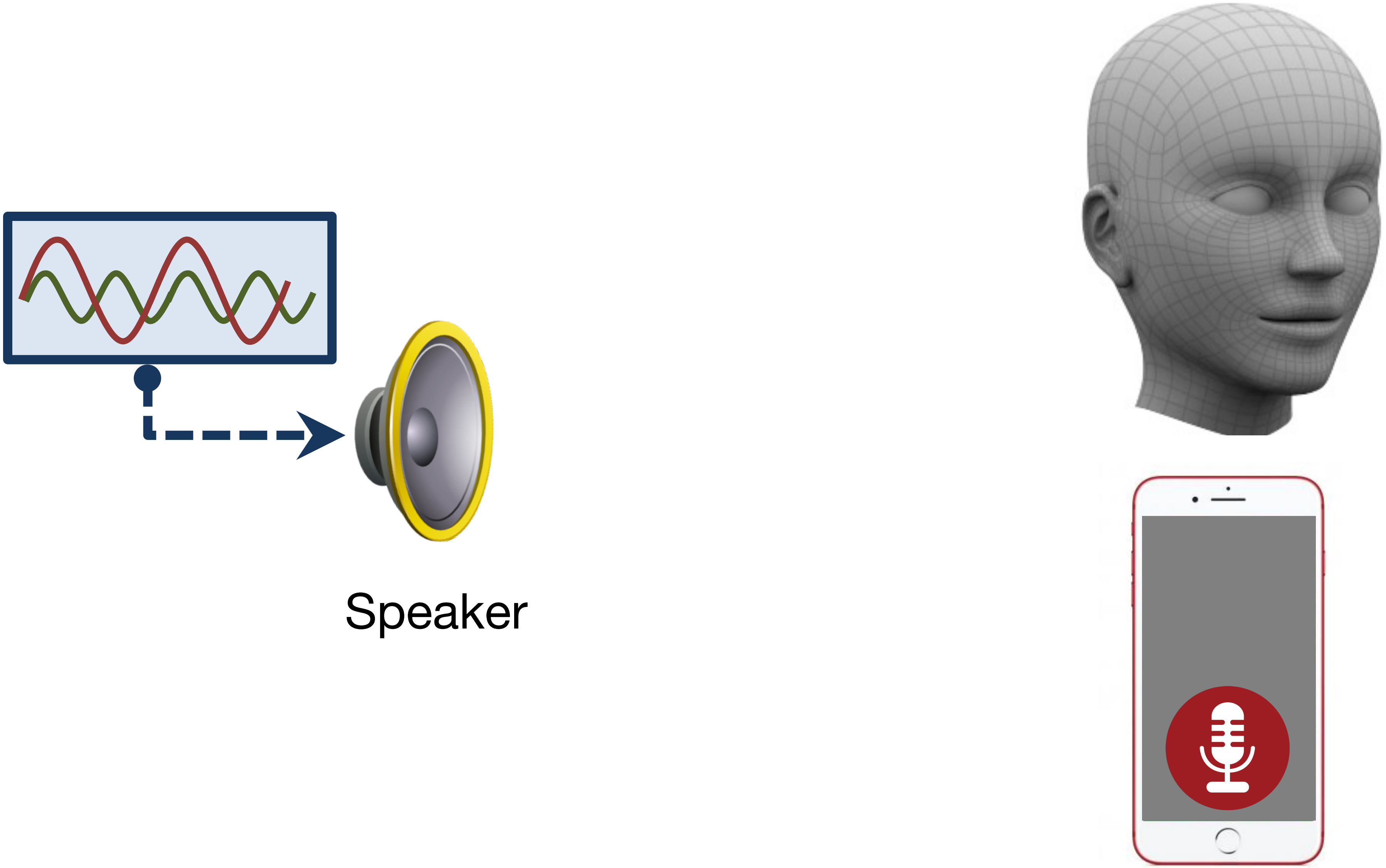
Microphones are everywhere



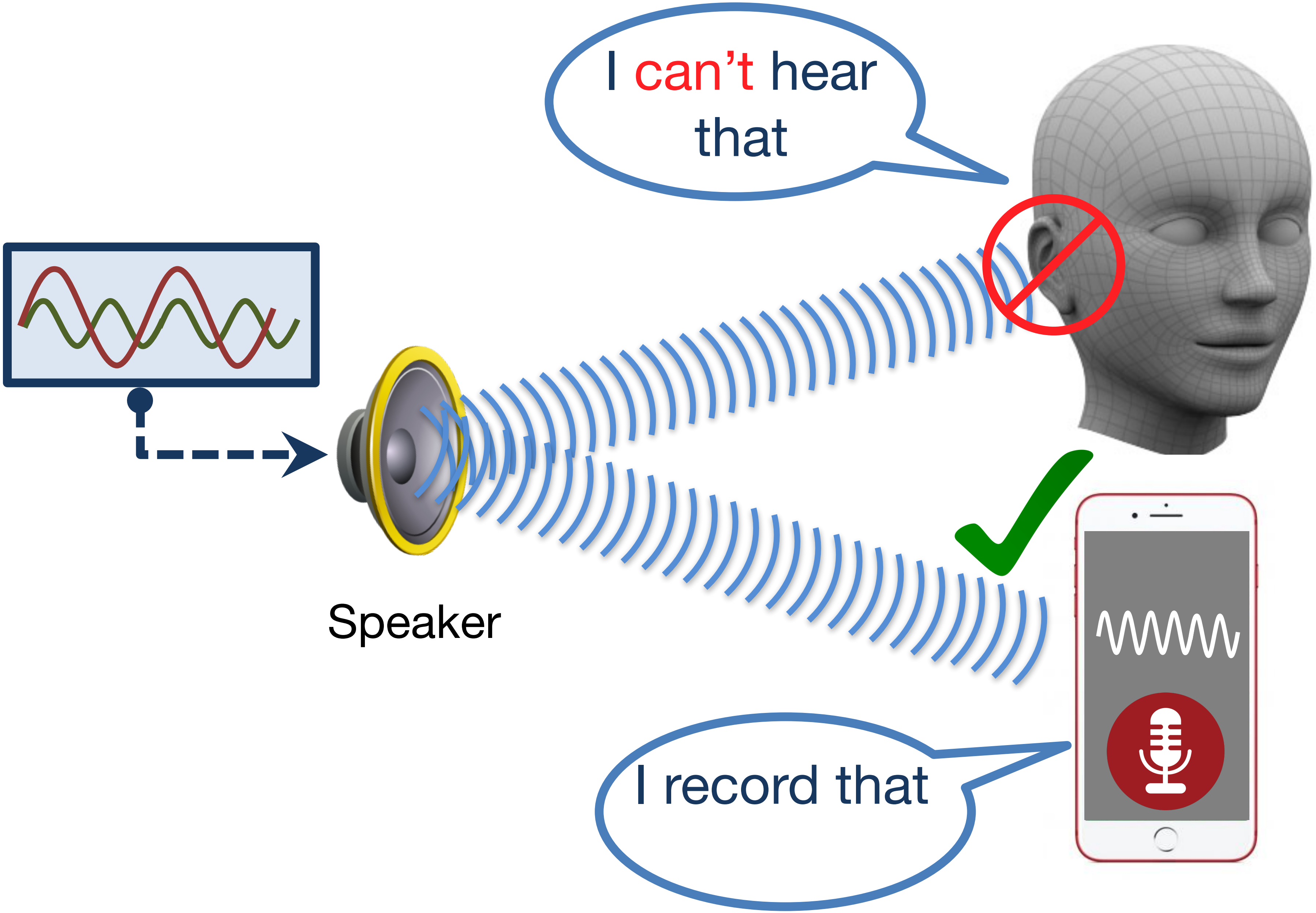
Microphones record audible sounds



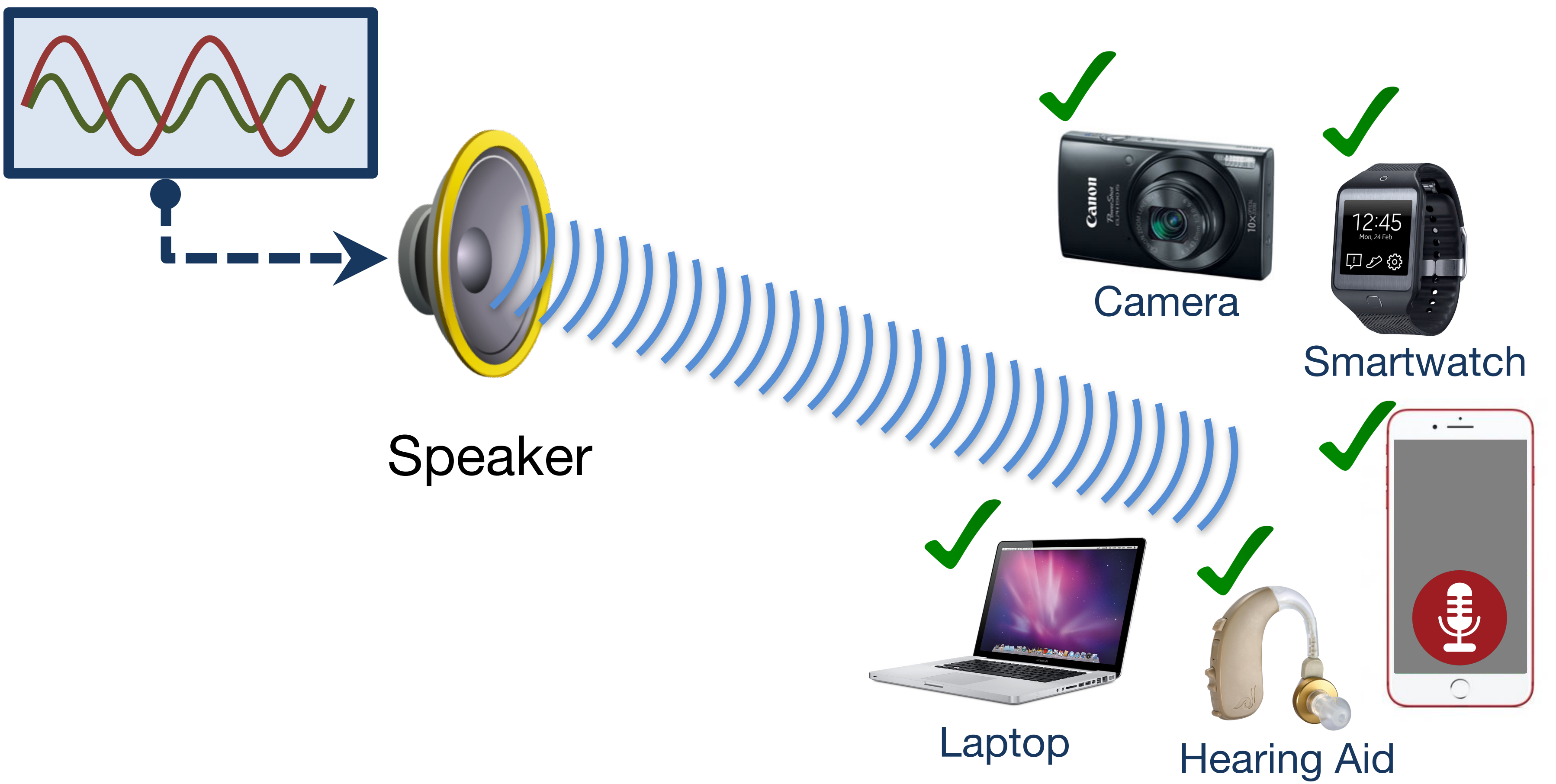
Inaudible, but recordable !



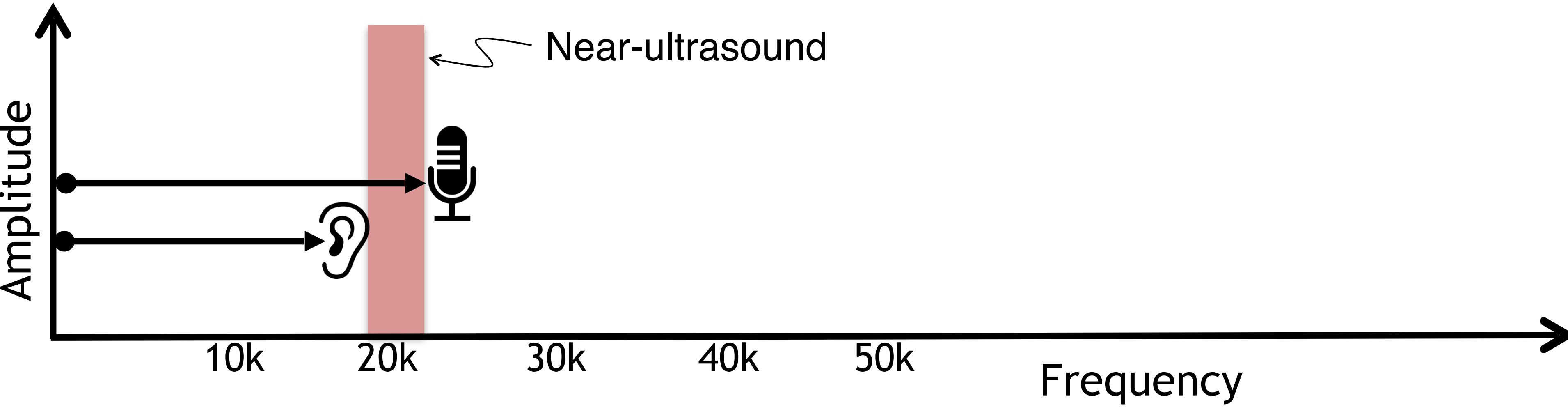
Inaudible, but recordable !



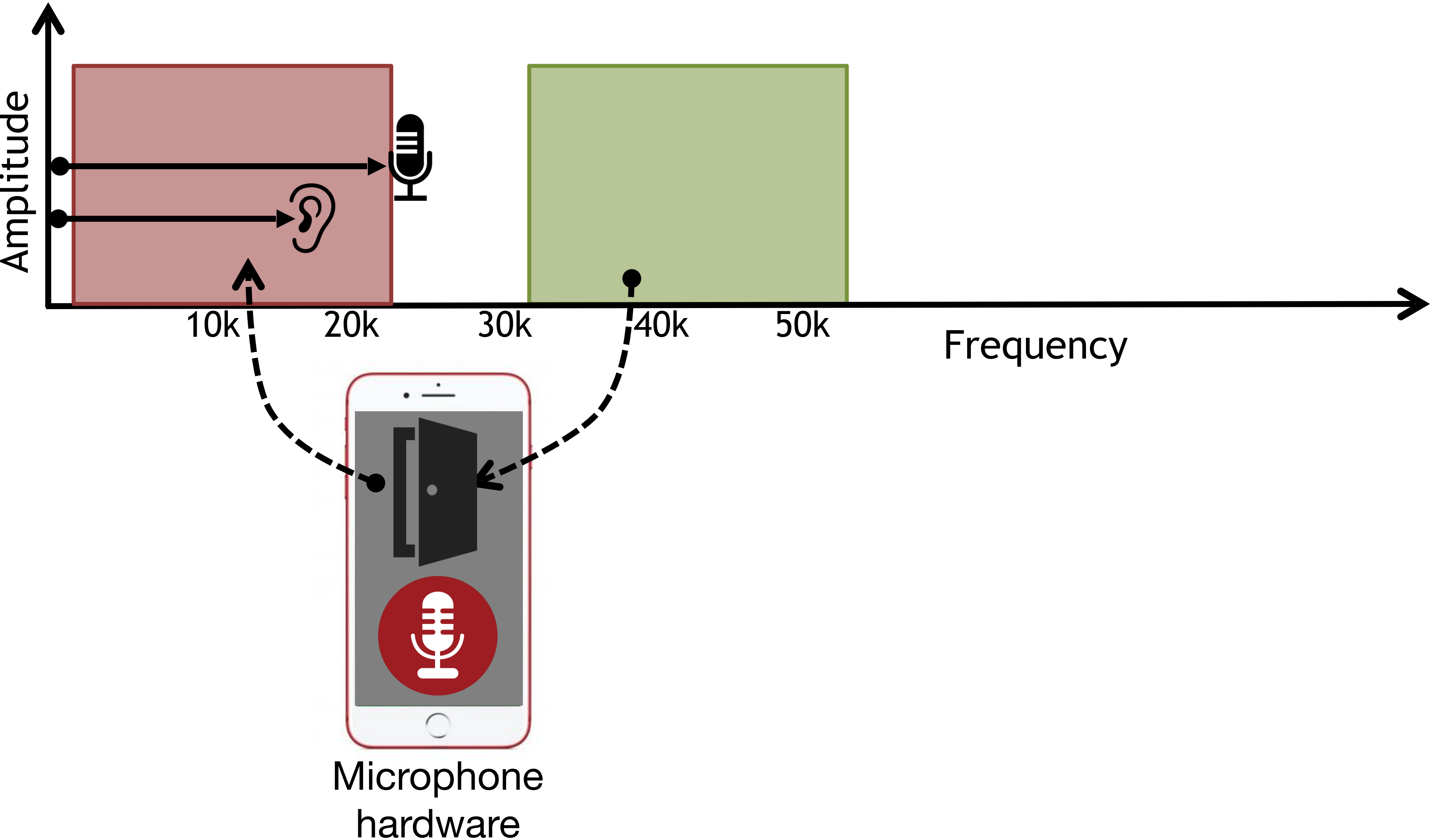
Works with unmodified devices



It’s not “near-ultrasound”



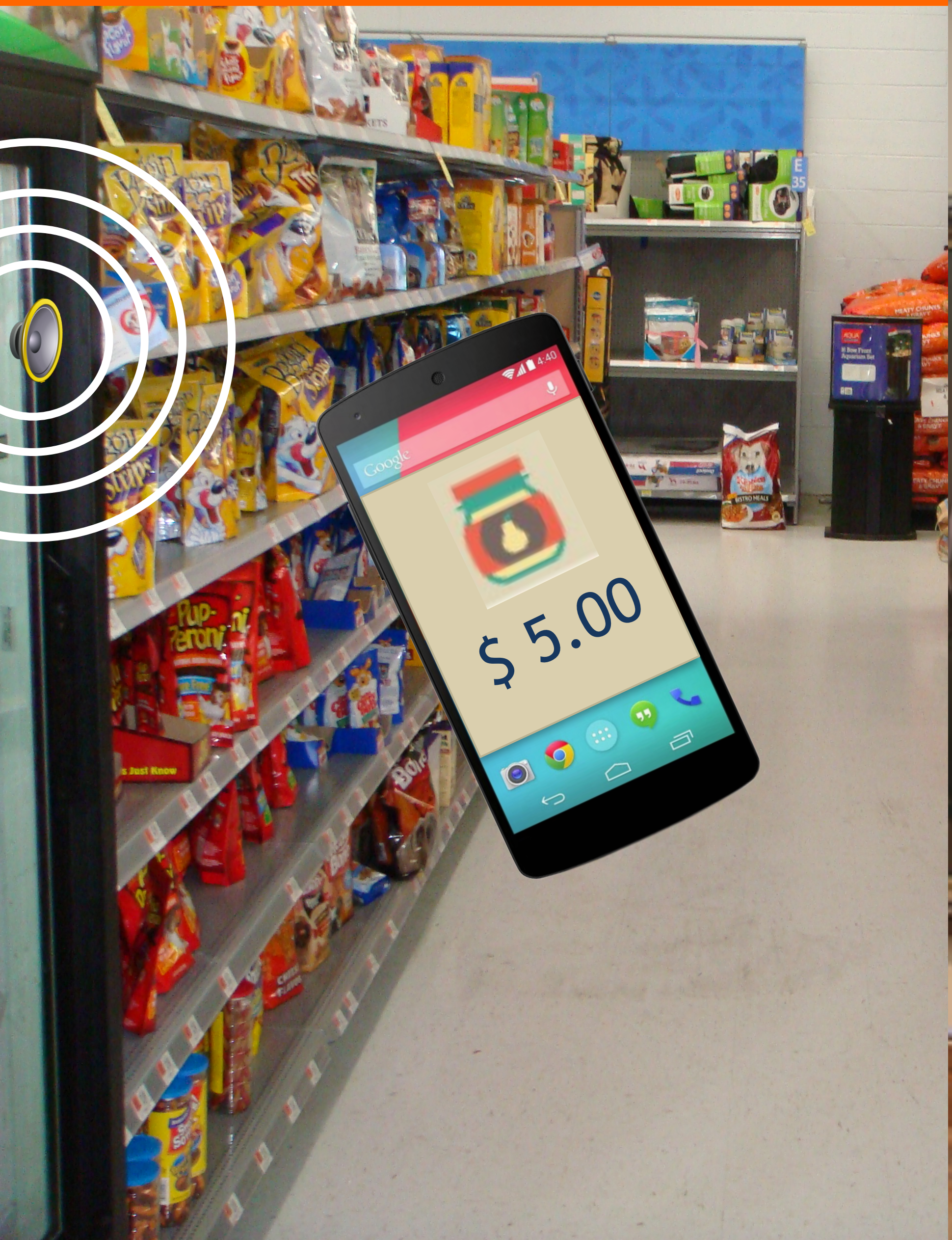
Exploiting fundamental nonlinearity



What can we do with it?

Application: Acoustic jammer

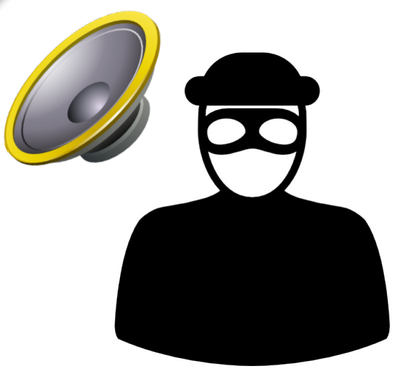
Application: Acoustic communication



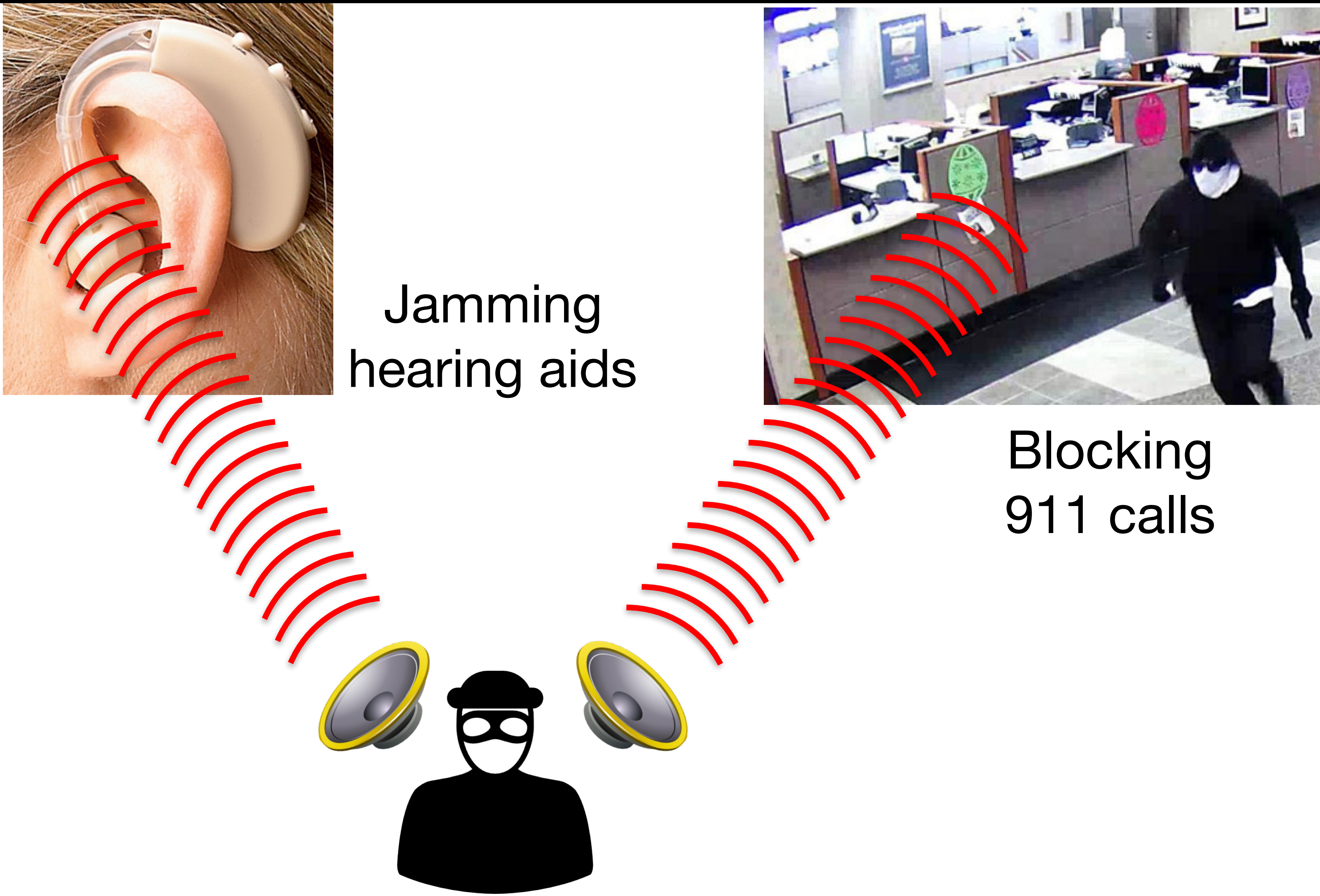
Threat: Acoustic DOS attack

Threat: Acoustic DOS attack

Jamming
hearing aids



Threat: Acoustic DOS attack



Talk outline

① Microphone Overview

② System Design

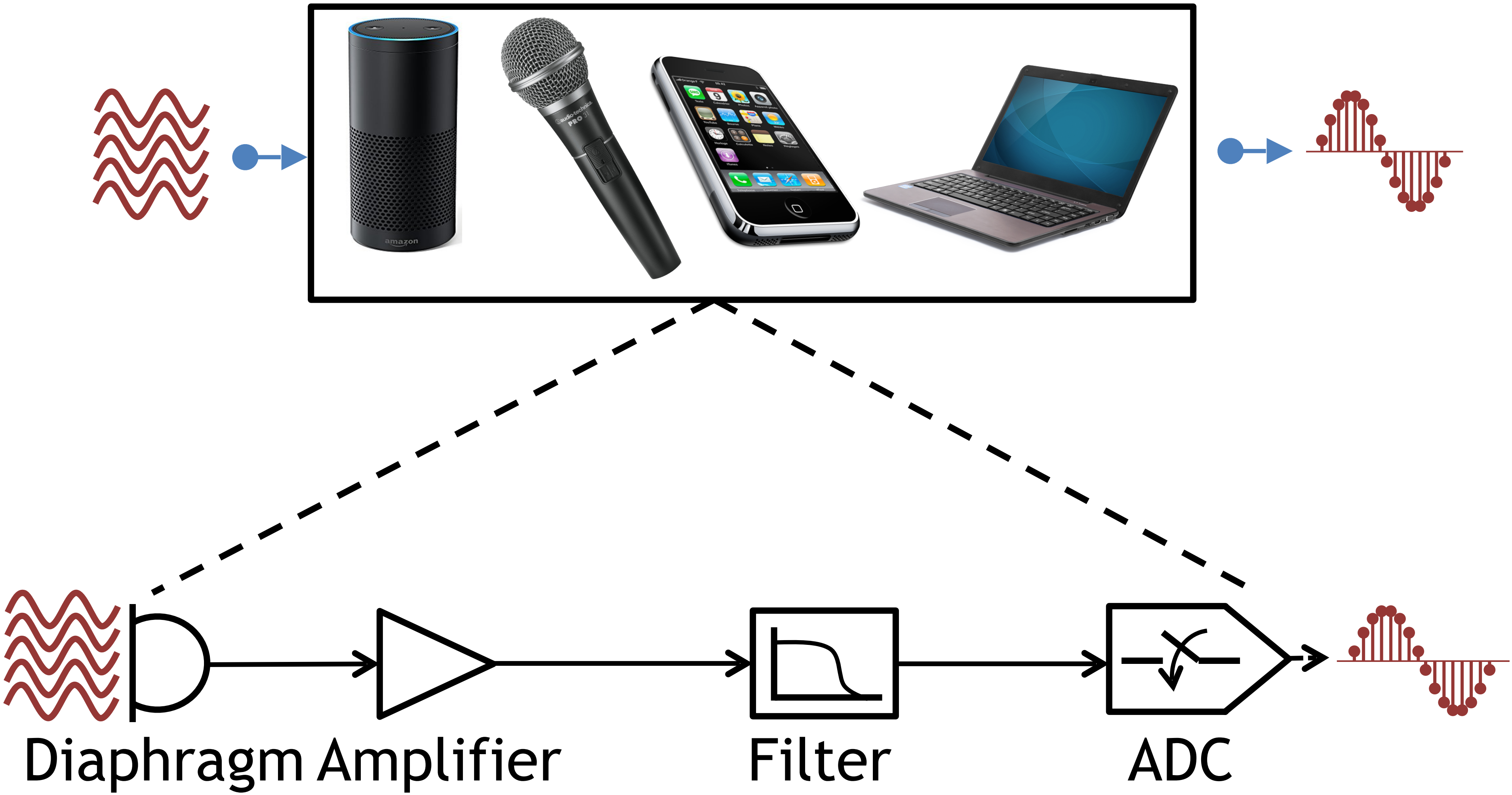
③ Challenges

④ Evaluation

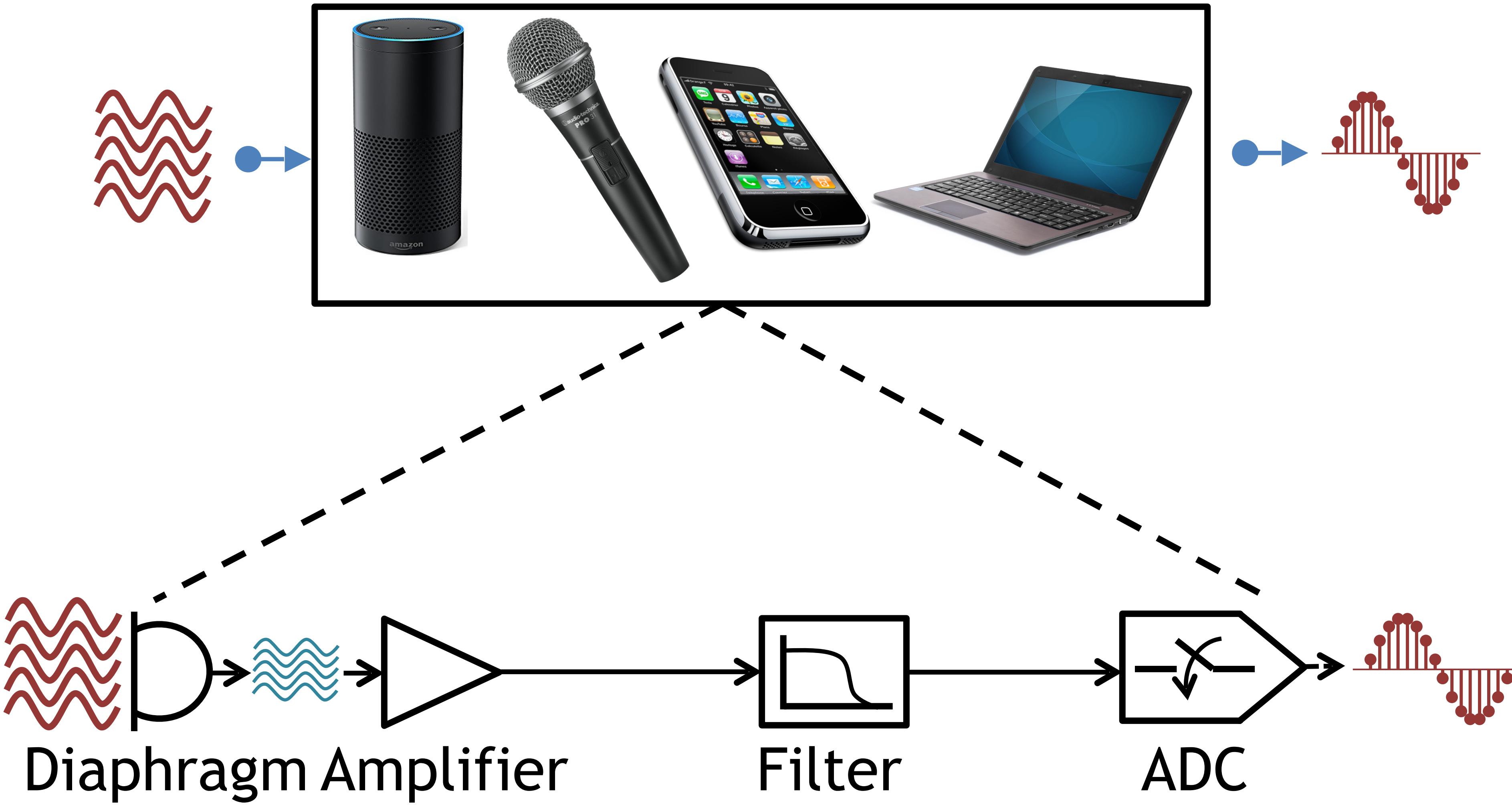
Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

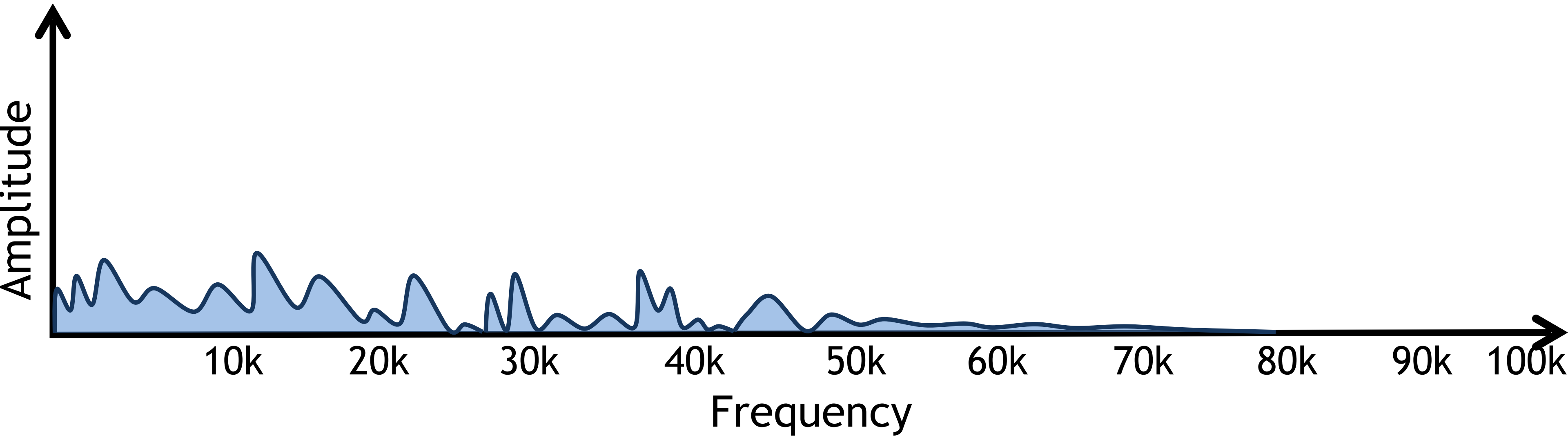
Microphone working principle

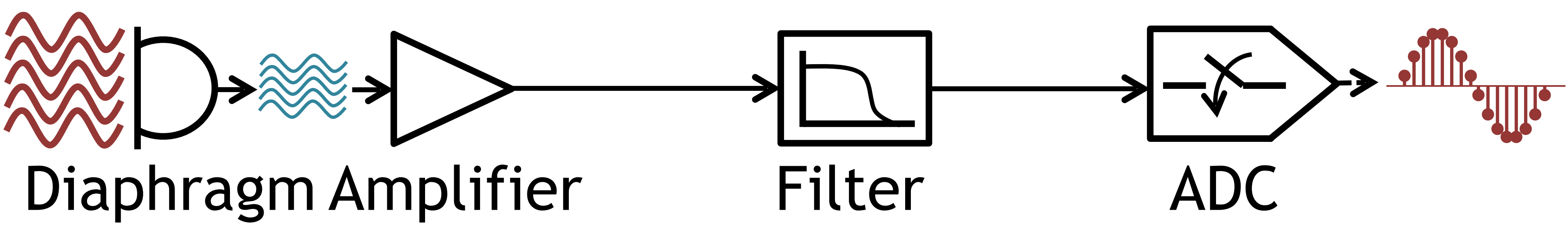


Microphone working principle

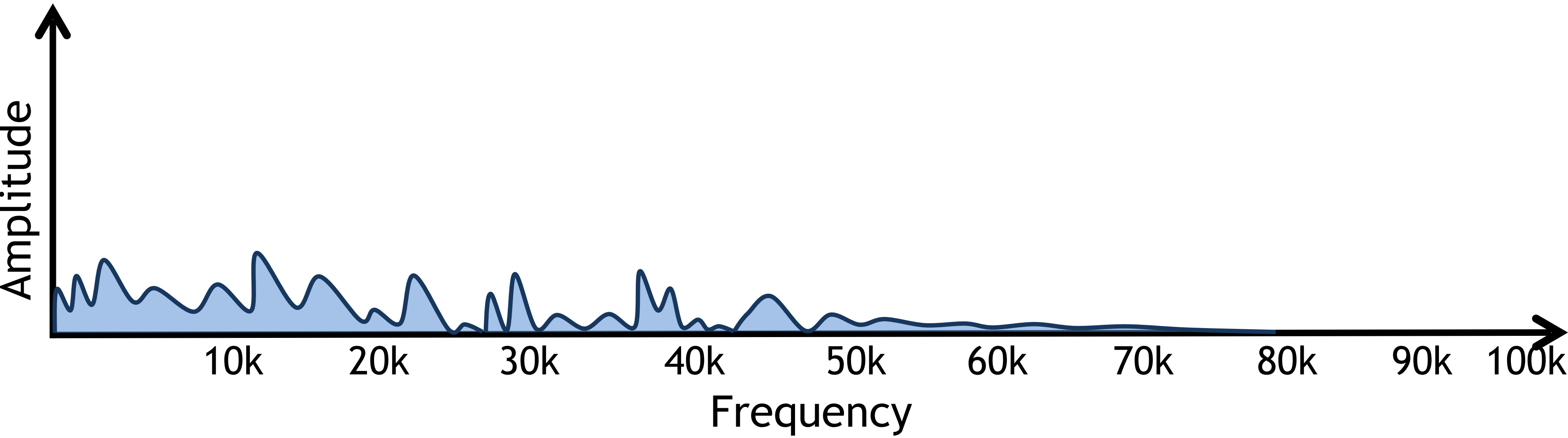


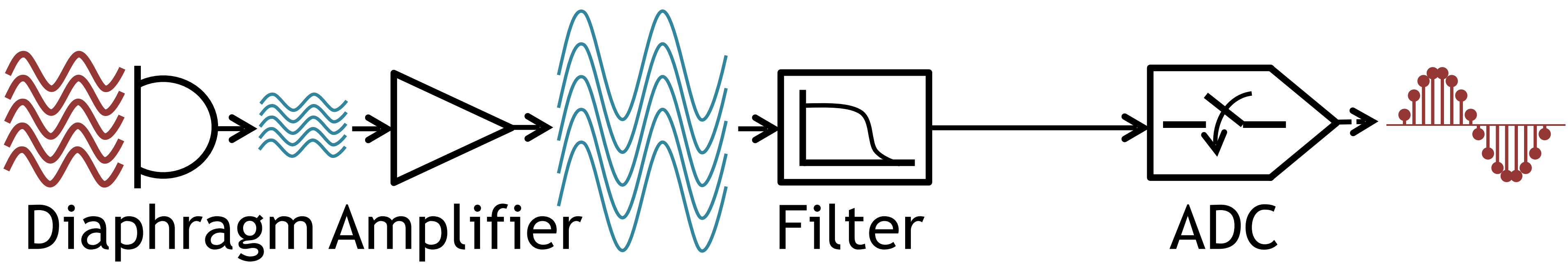
Microphone working principle



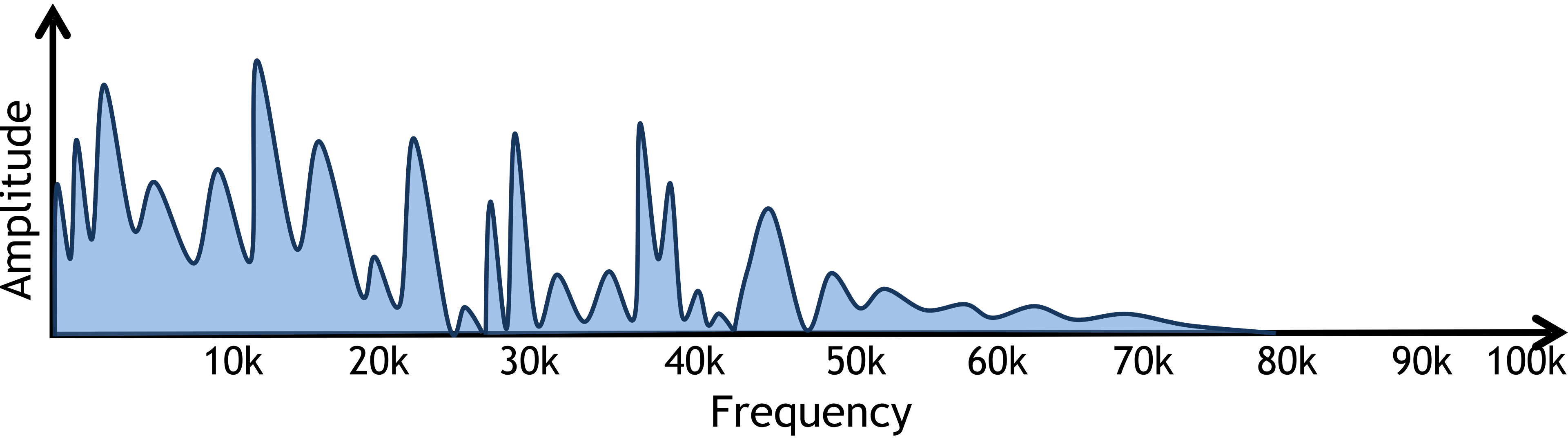


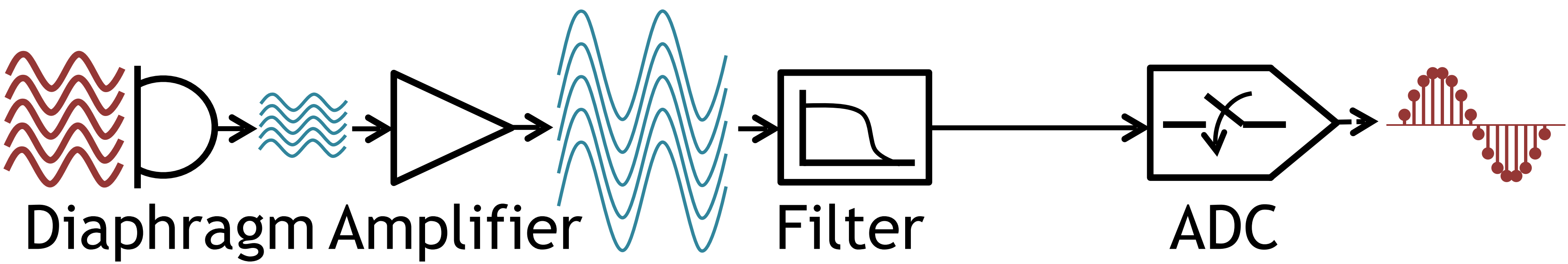
Microphone working principle



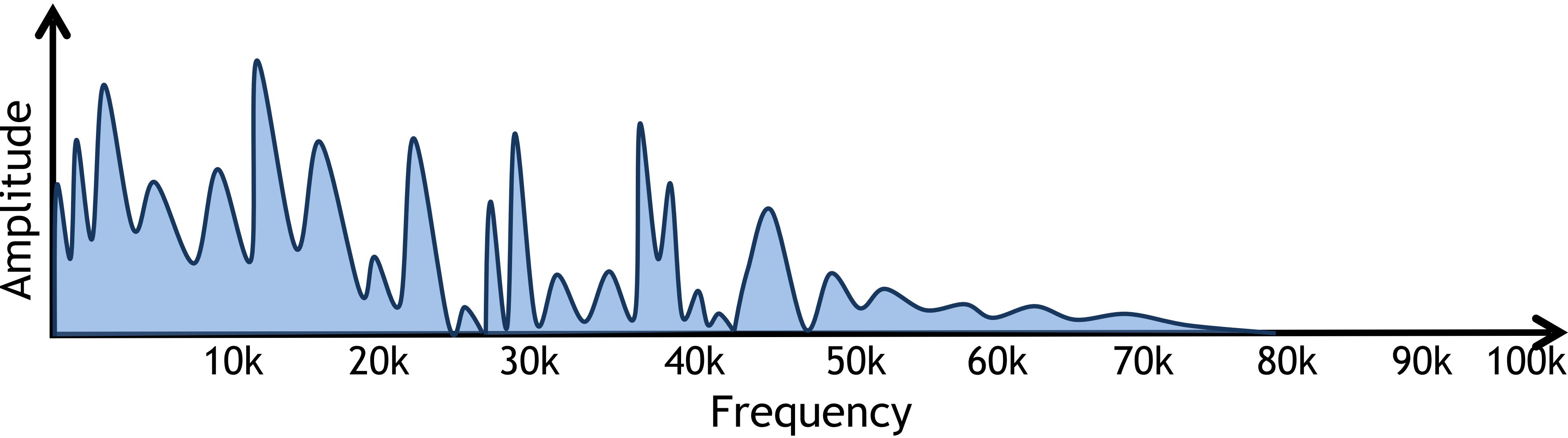


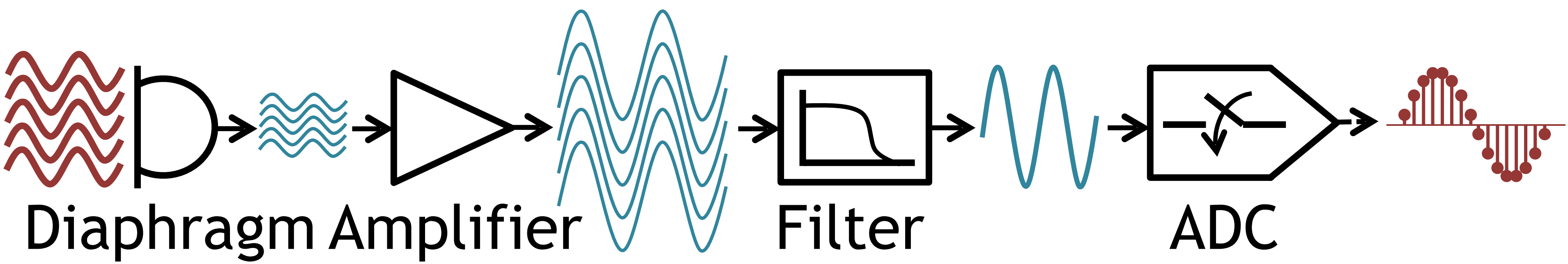
Microphone working principle



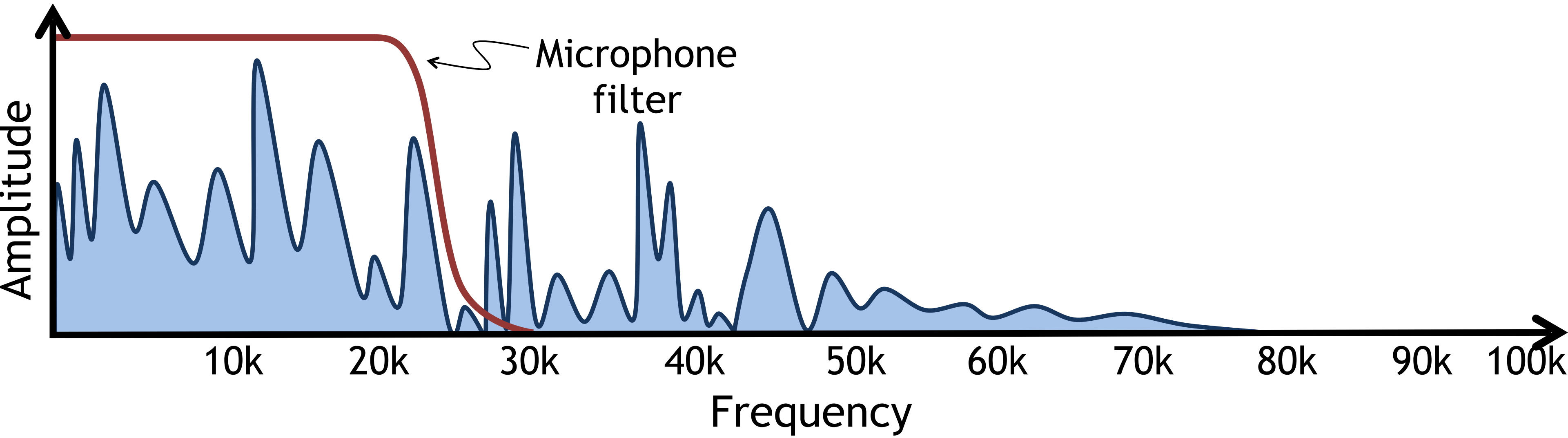


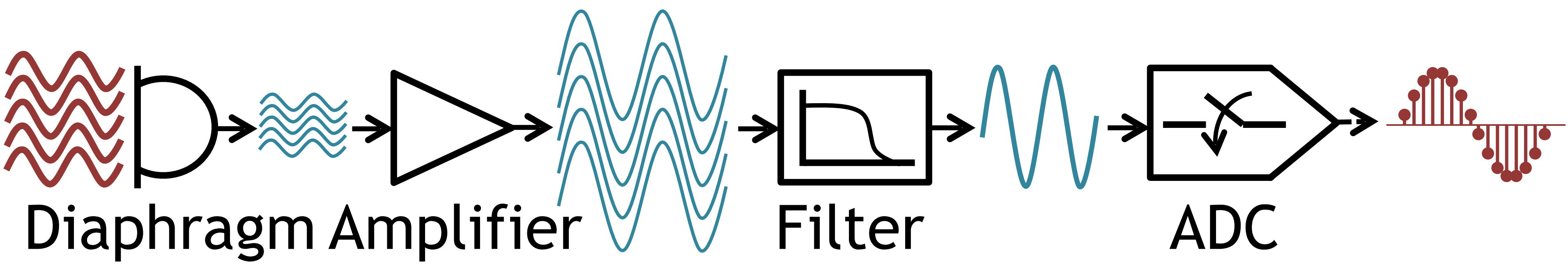
Microphone working principle



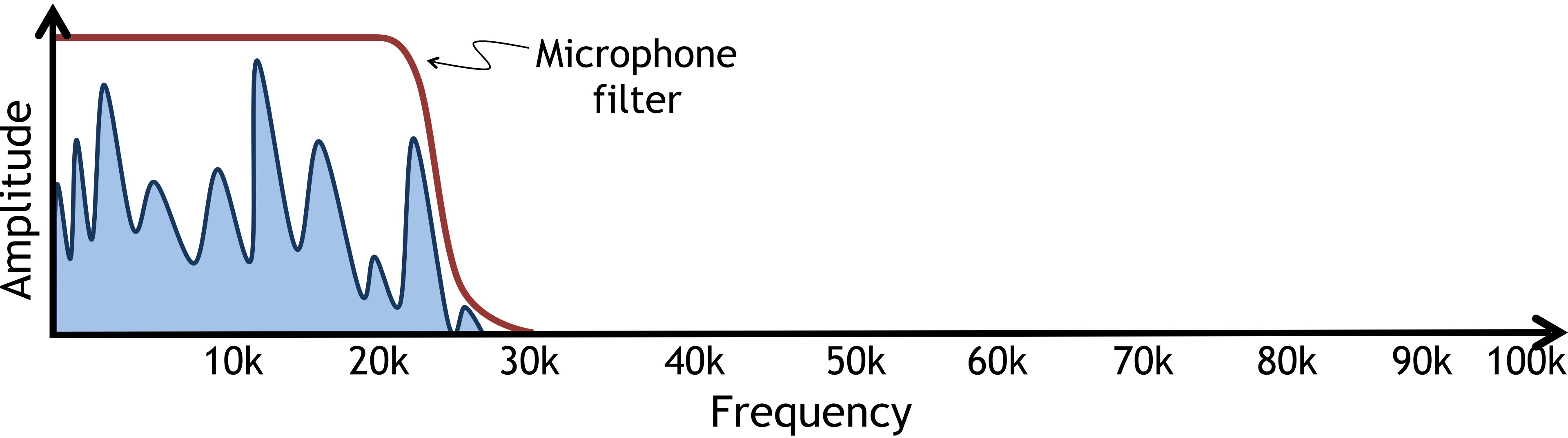


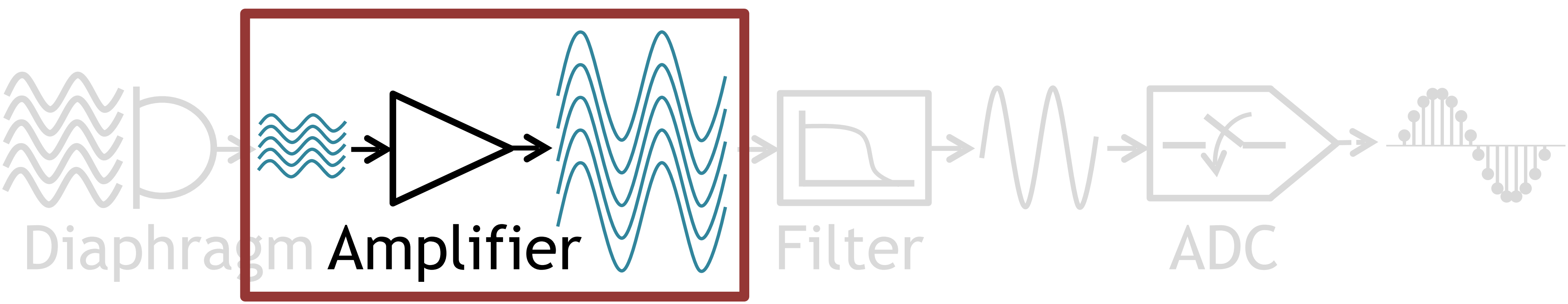
Microphone working principle



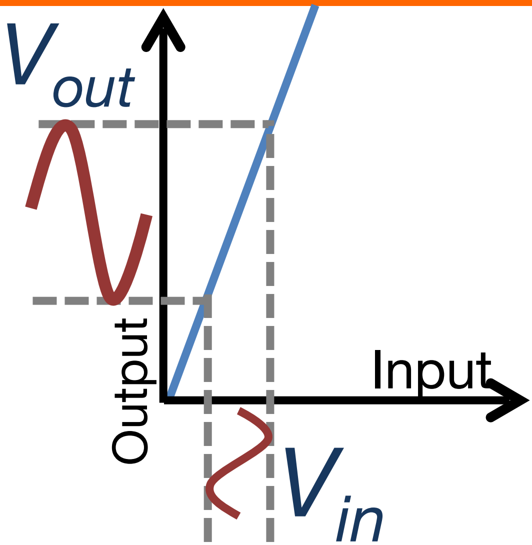


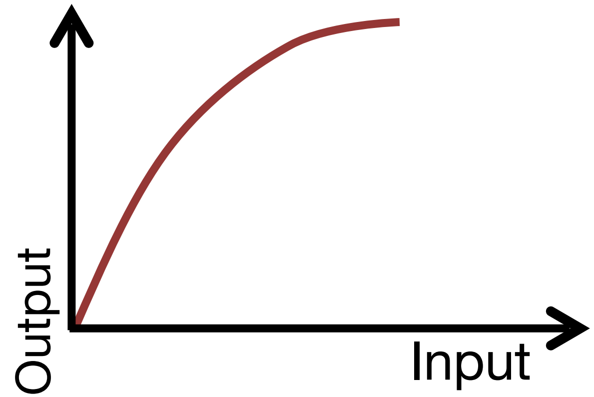
Microphone working principle





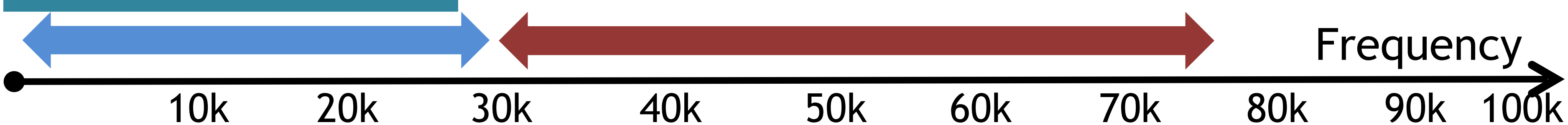
Microphone working principle

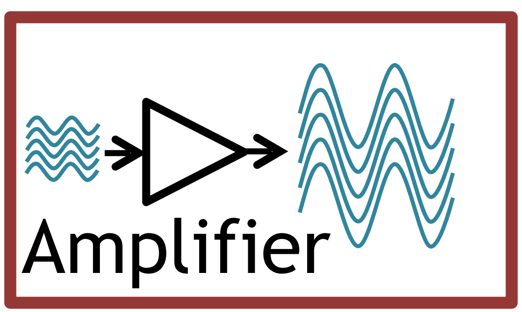




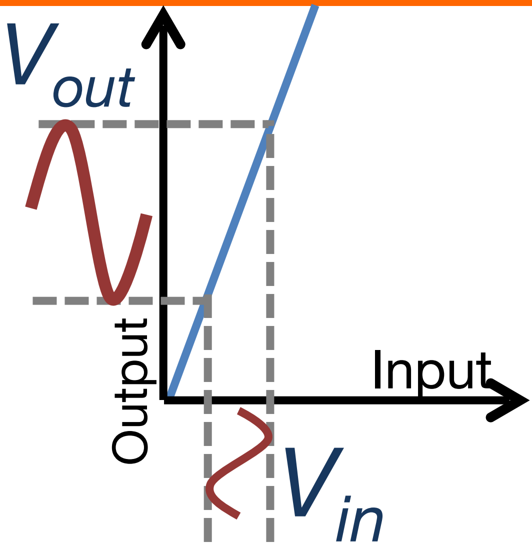
$$V_{out} = a_1 V_{in}$$

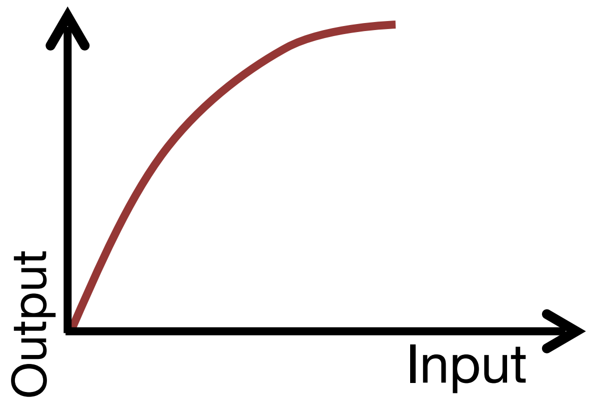
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$$





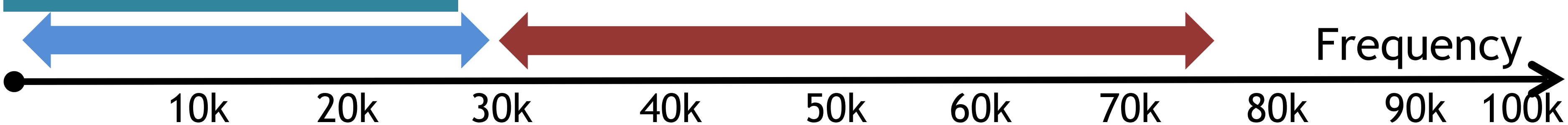
Microphone working principle

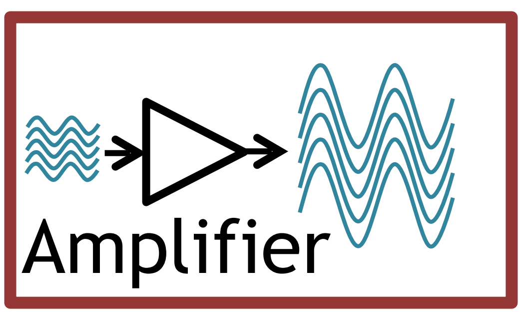




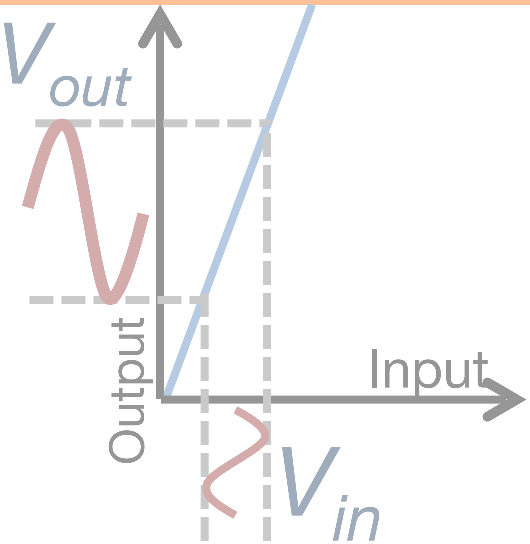
$$V_{out} = a_1 V_{in}$$

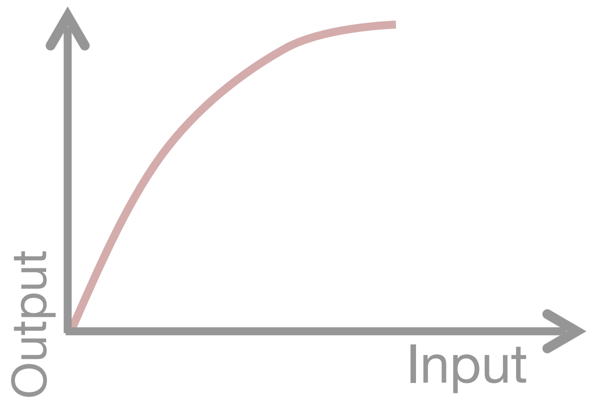
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$





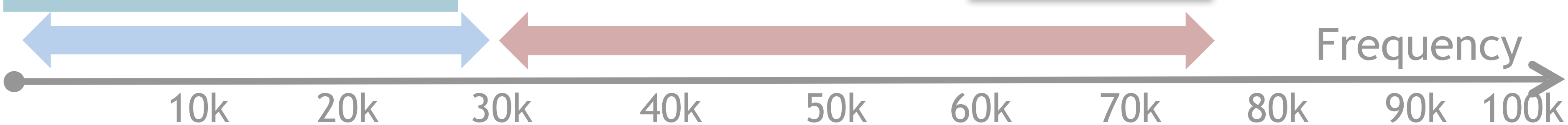
Microphone working principle

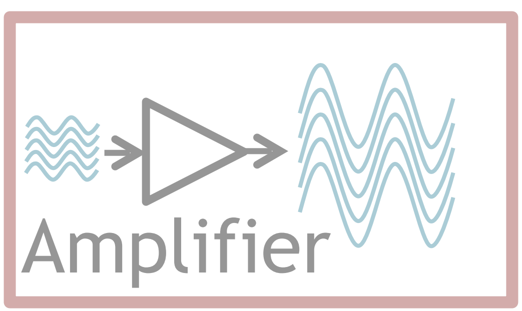




$$V_{out} = a_1 V_{in}$$

$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

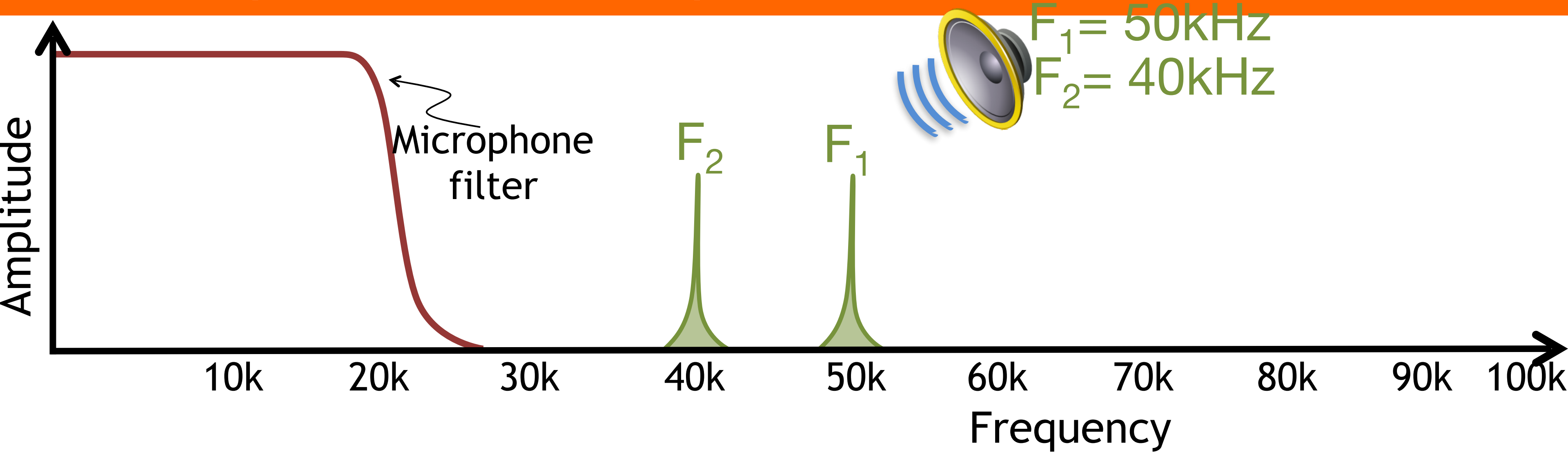




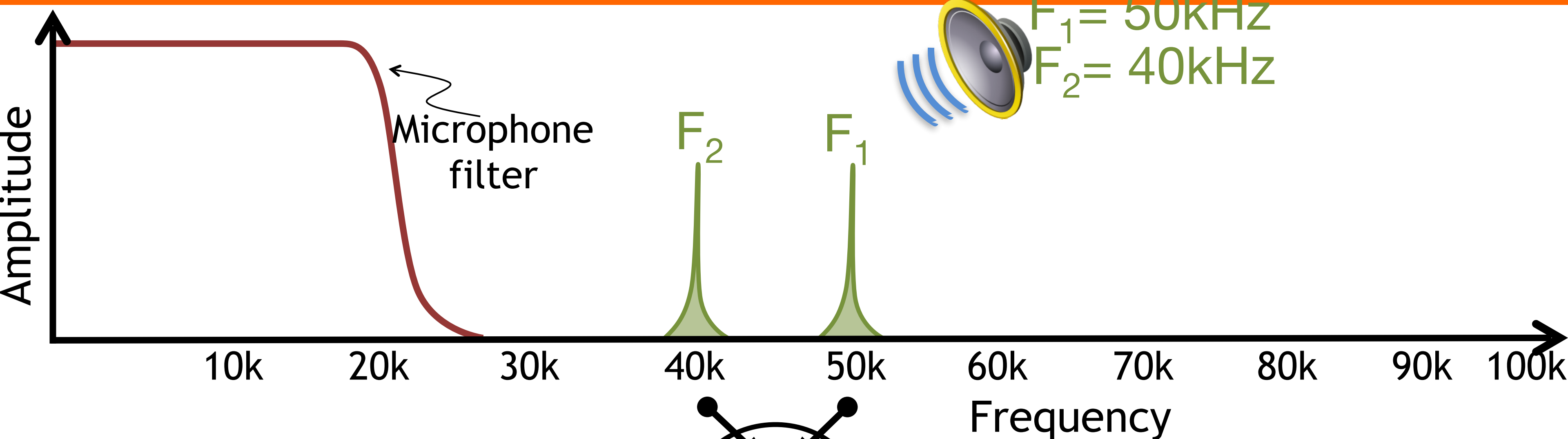
Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

Exploiting amplifier non-linearity



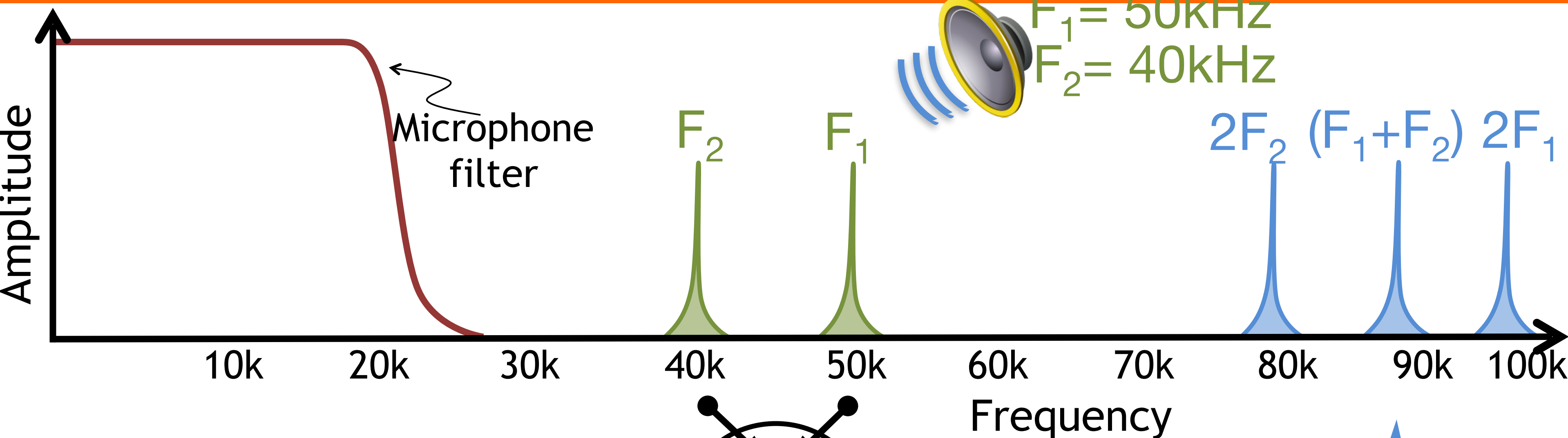
Exploiting amplifier non-linearity



$$V_{out} = a_1 V_{in} + a_2 V_{in}^{\,2}$$

$$\begin{aligned}(\sin F_1 + \sin F_2)^2 = \;& \cos 2F_1 \\ &+ \cos 2F_2 \\ &+ \cos (F_1 + F_2) \\ &+ \cos (F_1 - F_2)\end{aligned}$$

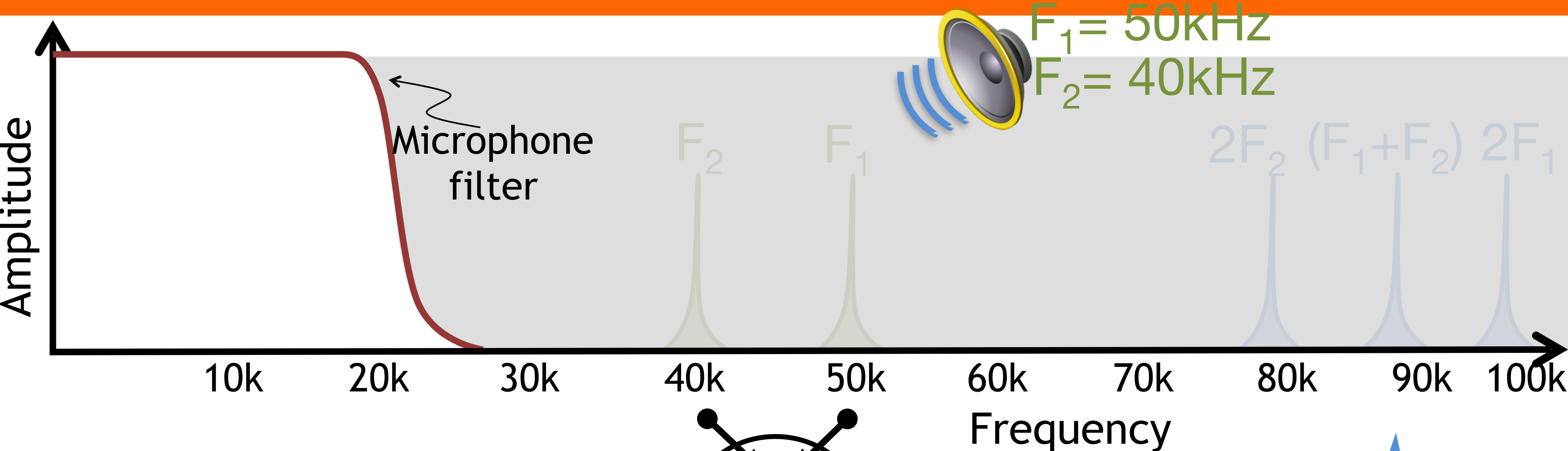
Exploiting amplifier non-linearity



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 = \cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

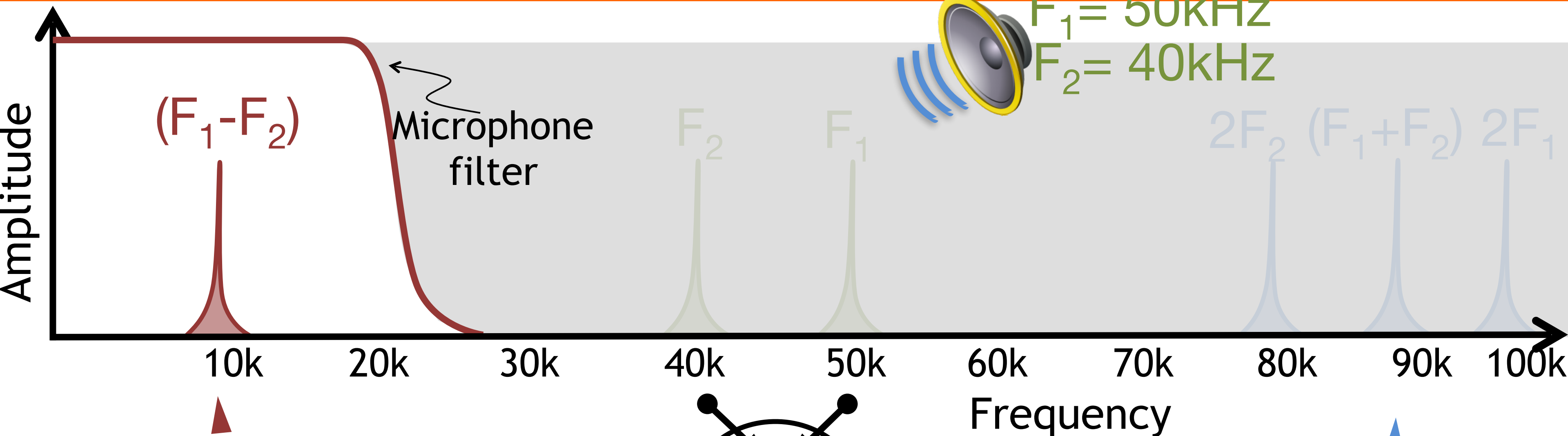
Exploiting amplifier non-linearity



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 = \cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

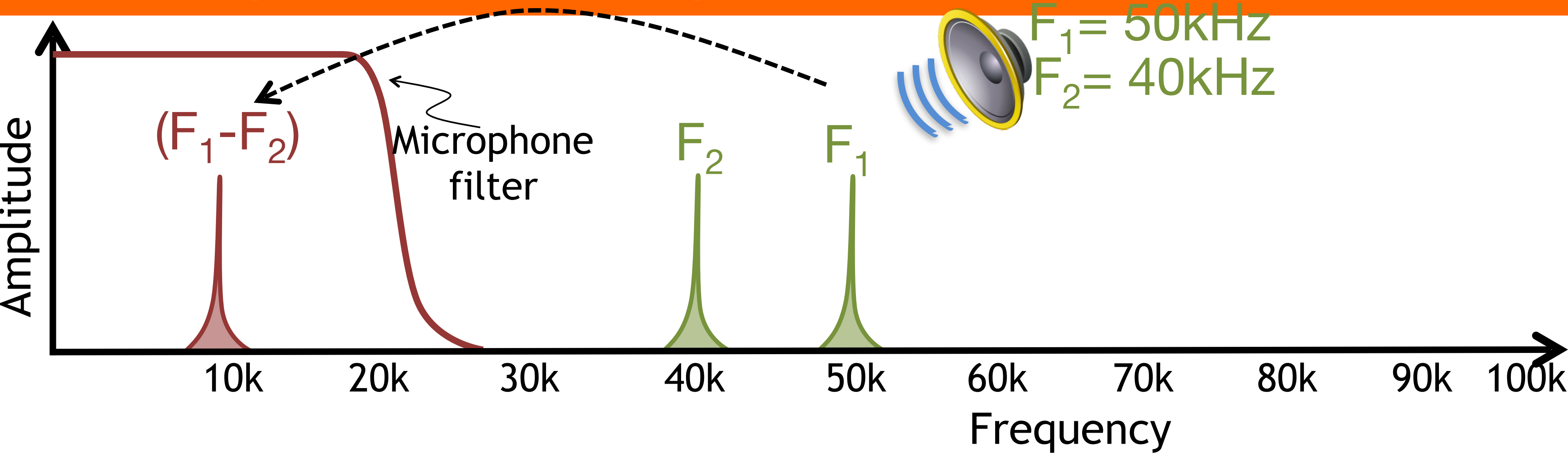
Exploiting amplifier non-linearity



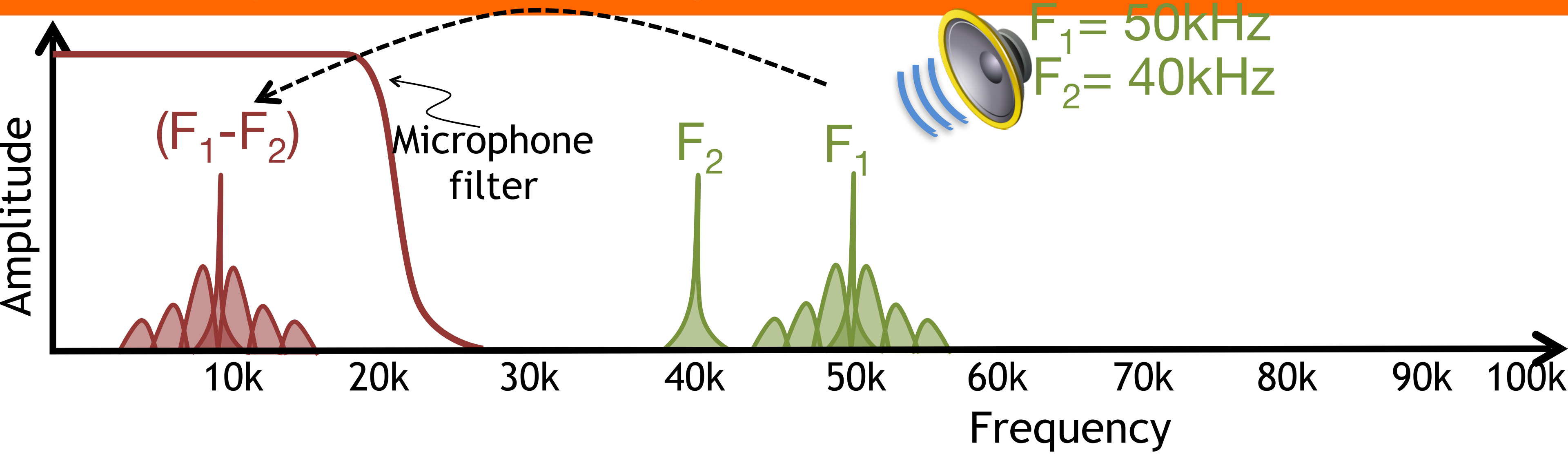
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 = \cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

Exploiting amplifier non-linearity



Exploiting amplifier non-linearity

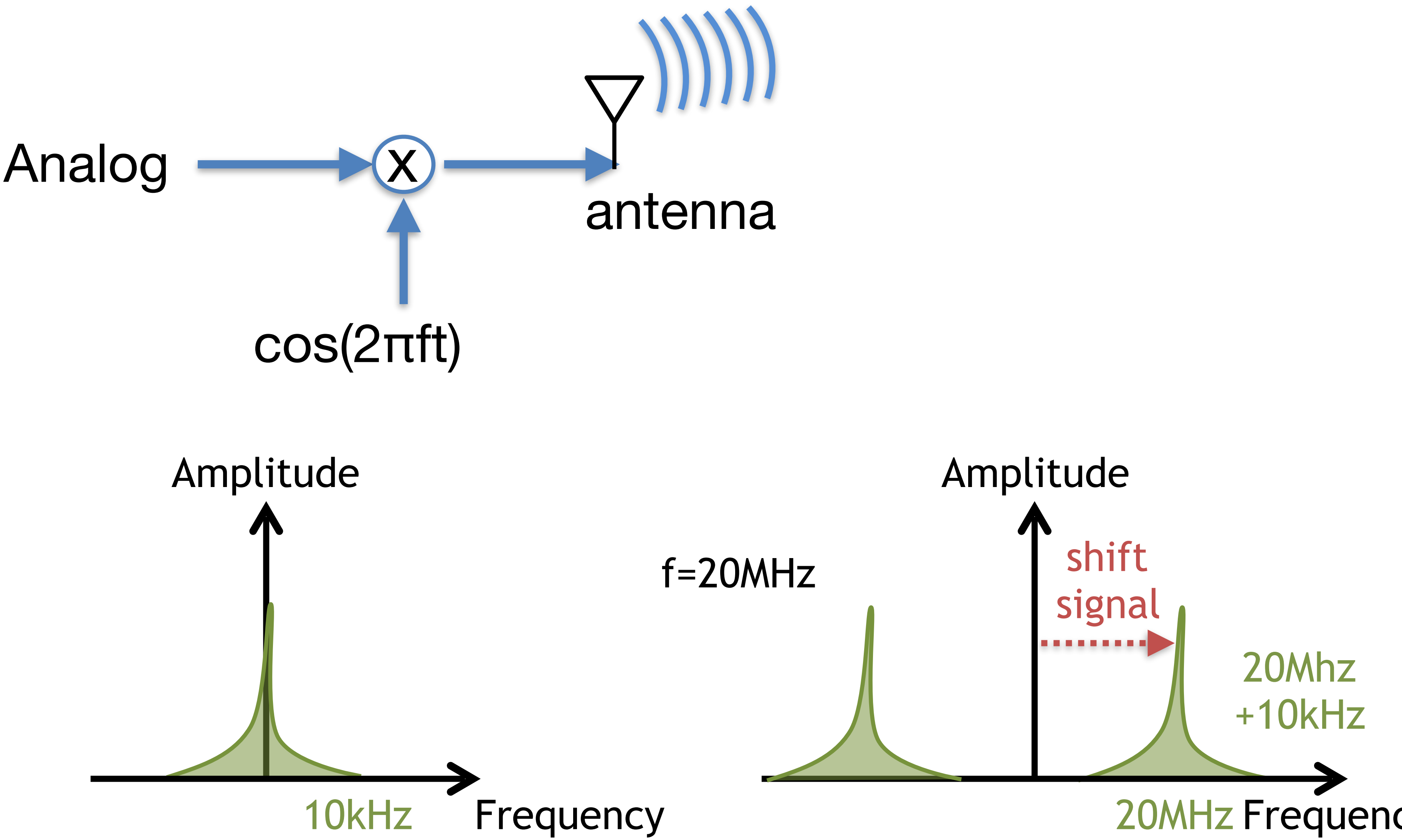


Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

Reminder of Modulation

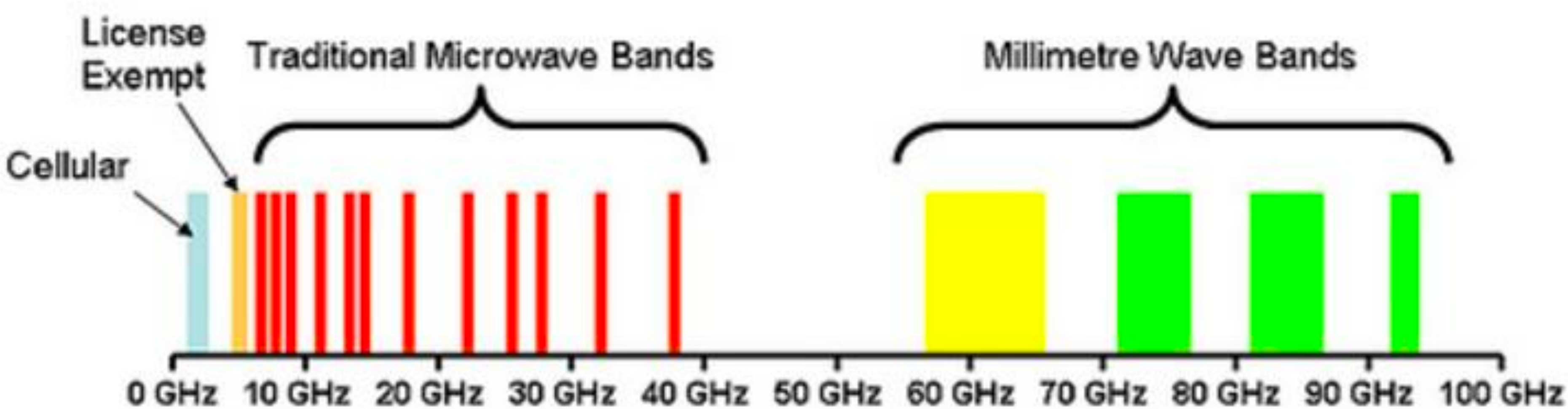
Modulation



Analog
x
antenna
cos(2πft)
Amplitude
10kHz
Frequency
f=20MHz
Amplitude
shift
signal
20Mhz
+10kHz
20MHz
Frequenc

Why is Modulation useful?

1. Interference, Technology Co-existence
2. Spectrum Access (Legal)
3. Antenna size (wavelength/4)

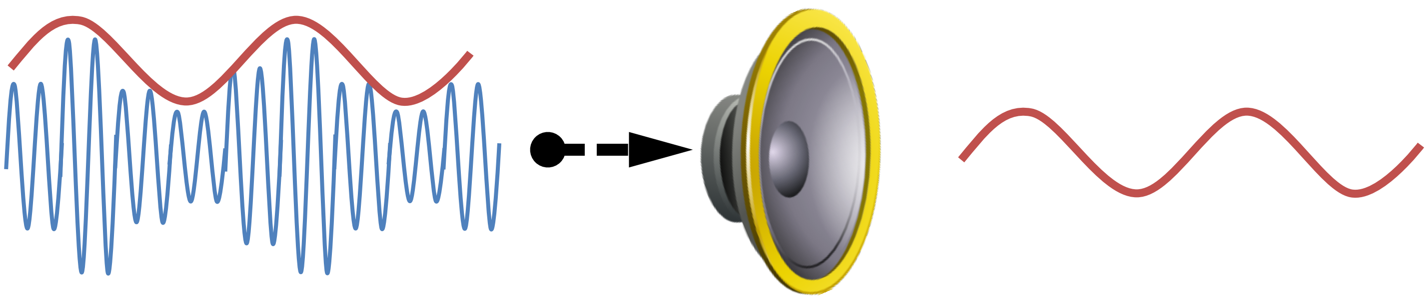


WiFi? LTE? 5G?

Challenges

~~Amplitude modulation~~

$$S_{AM} = a \cdot \underbrace{\sin(\omega_m t)}_{\text{message}} \cdot \underbrace{\sin(\omega_c t)}_{\text{carrier}}$$



Ultrasonic speaker

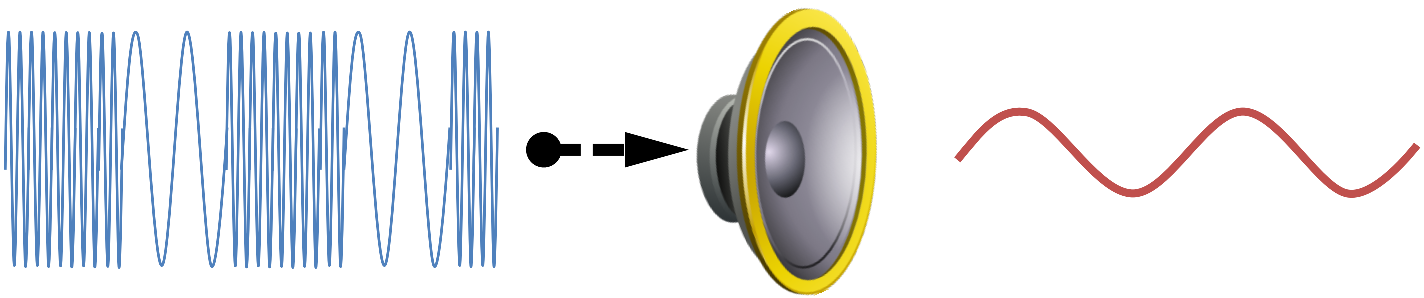
$$\begin{aligned}
S^2_{out,AM} &= A_2\{aSin(\omega_m t).Sin(\omega_c t)\}^2 \\
&= -A_2\frac{a^2}{4}\{Cos(\omega_c t - \omega_m t) - Cos(\omega_c t + \omega_m t)\}^2 \\
&= -A_2\frac{a^2}{4}Cos(2\omega_m t) + (terms\ with\ frequencies \\
&\qquad above\ \omega_c\ and\ DC)
\end{aligned}$$

Problem: speaker has non-linearities => Audible sound

Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$

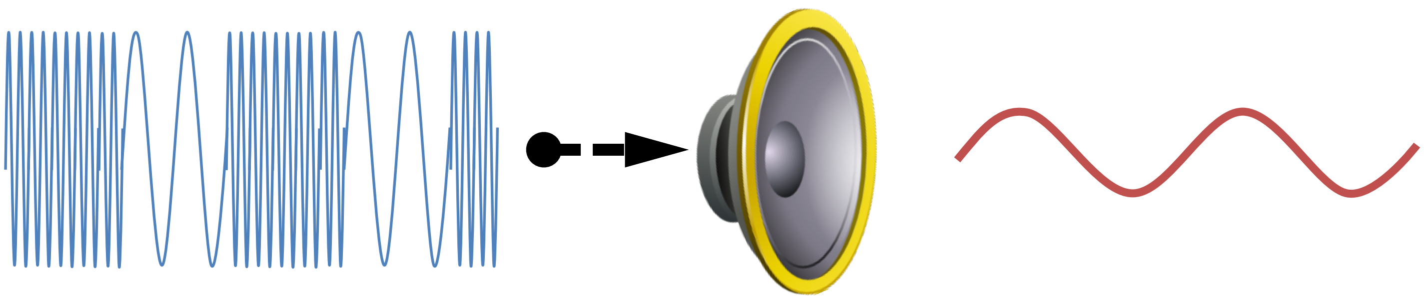


Ultrasonic speaker

Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$

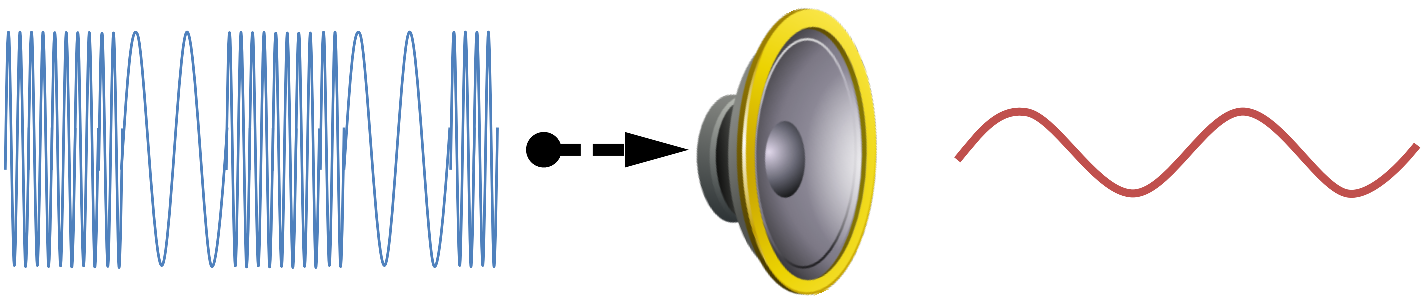


Ultrasonic speaker

Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



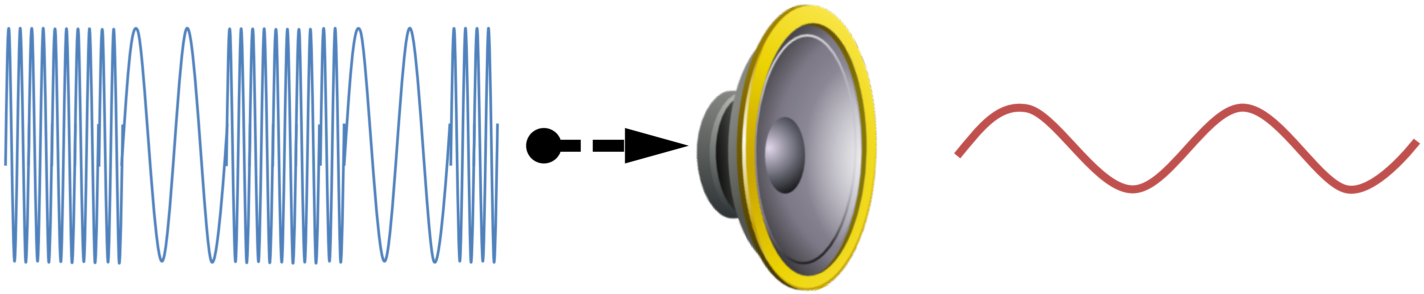
Ultrasonic speaker

$$S_{FM}^2 \sim 1 + \cos(2\omega_c t + \text{ other terms })$$

Problem: microphone can't measure inaudible sound

Solution?

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



Ultrasonic
speaker

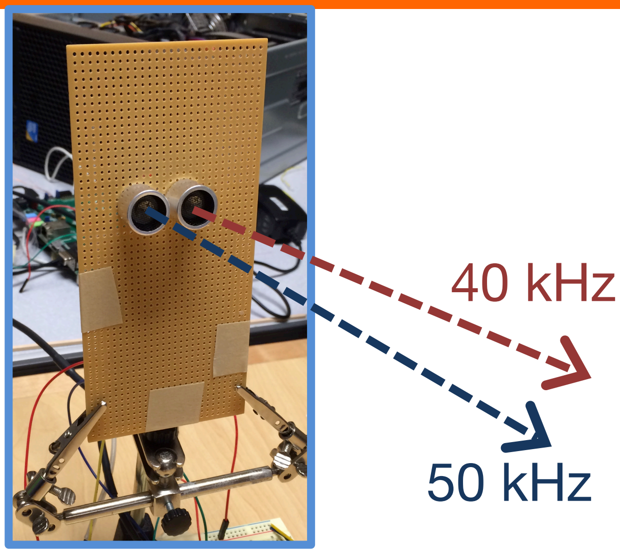
Add another speaker

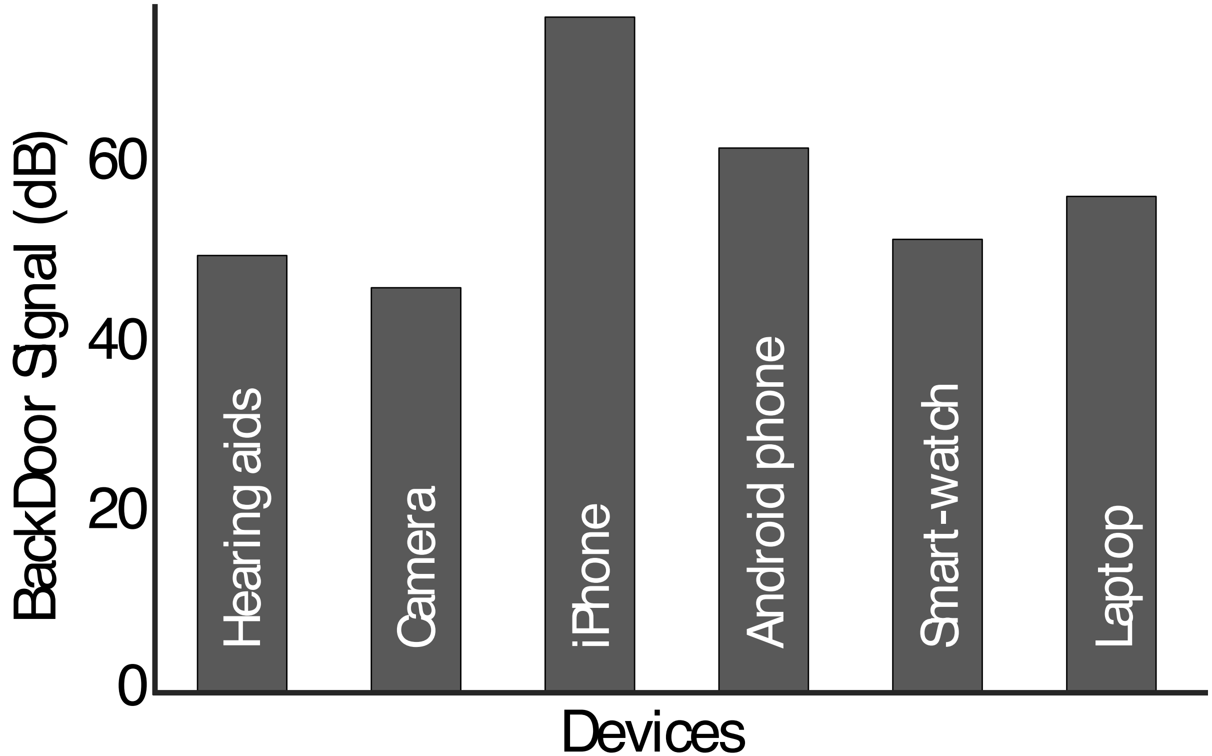
How do we structure its signal?

Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

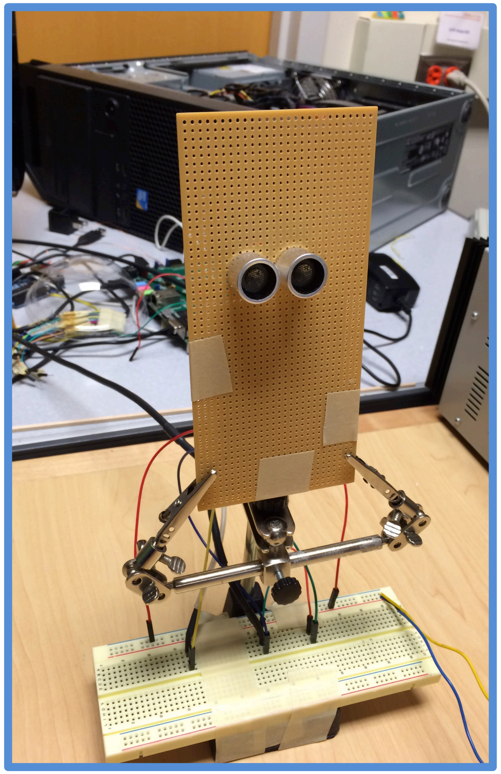
Hardware generalizability



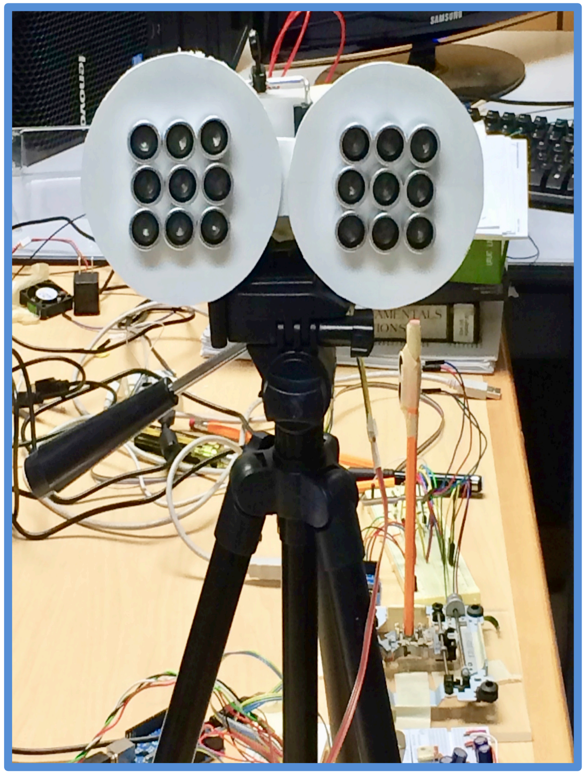


Hearing Aid | Camera | iPhone | Android phone | Smartwatch | Laptop

Implementation

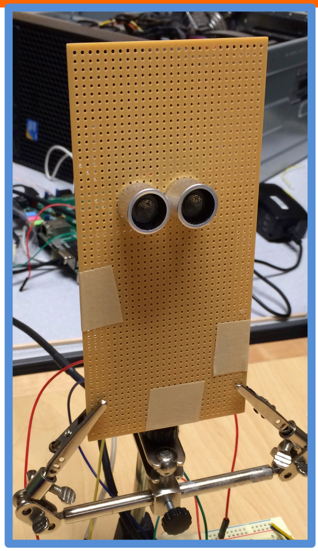


Communication
prototype



Jammer
prototype

Communication performance



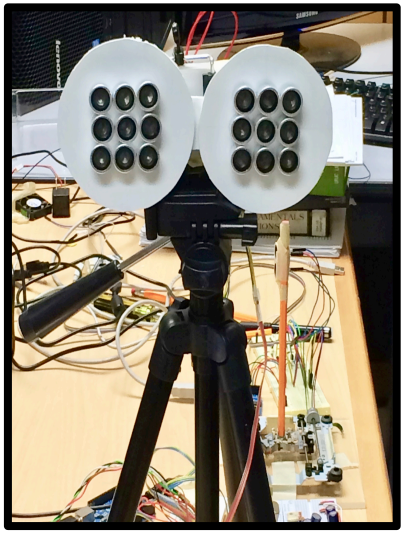
FM data packets

4kbps
up to 1 meter

More power can increase the distance

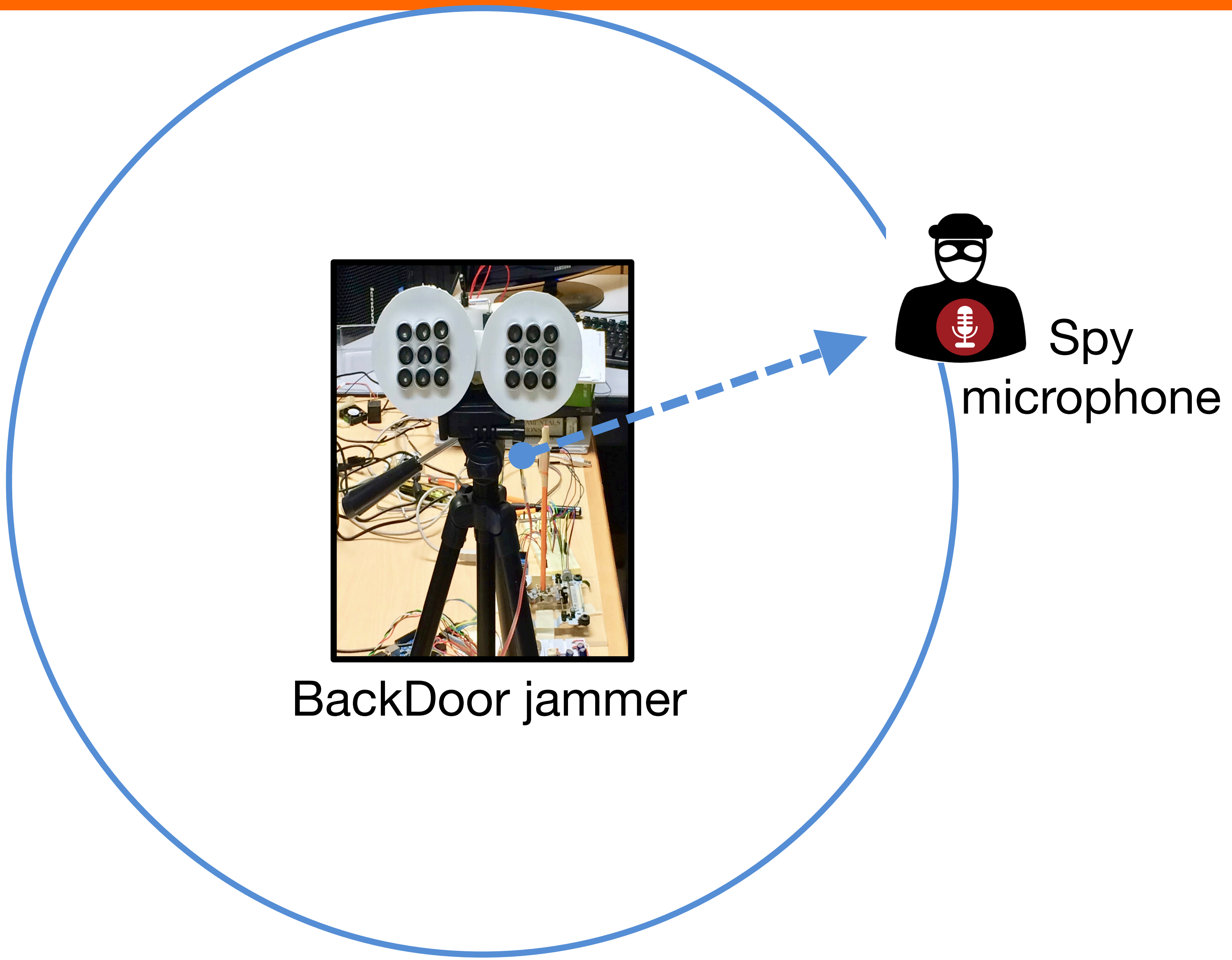
Jamming performance

Spy microphone

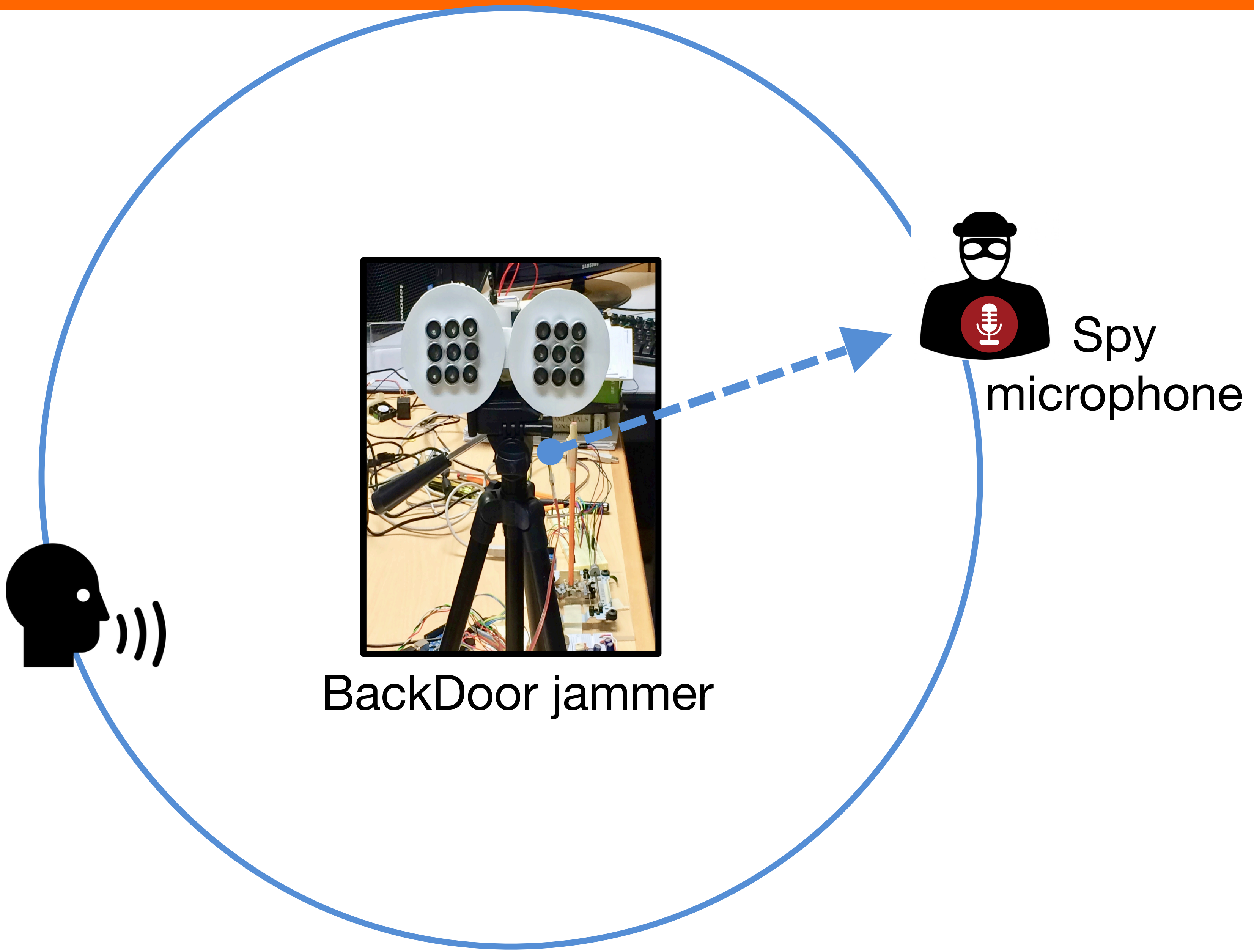


BackDoor jammer

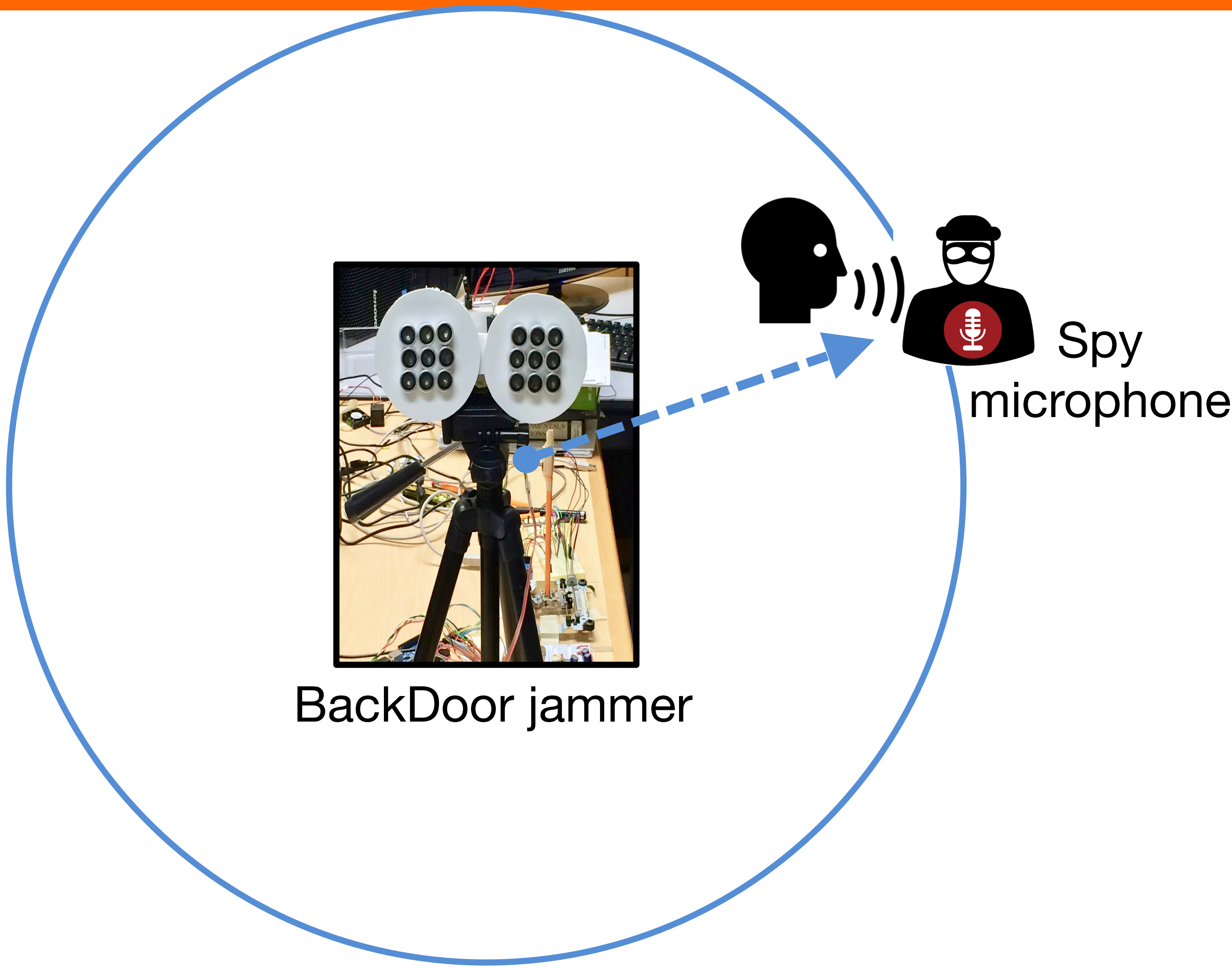
Jamming performance



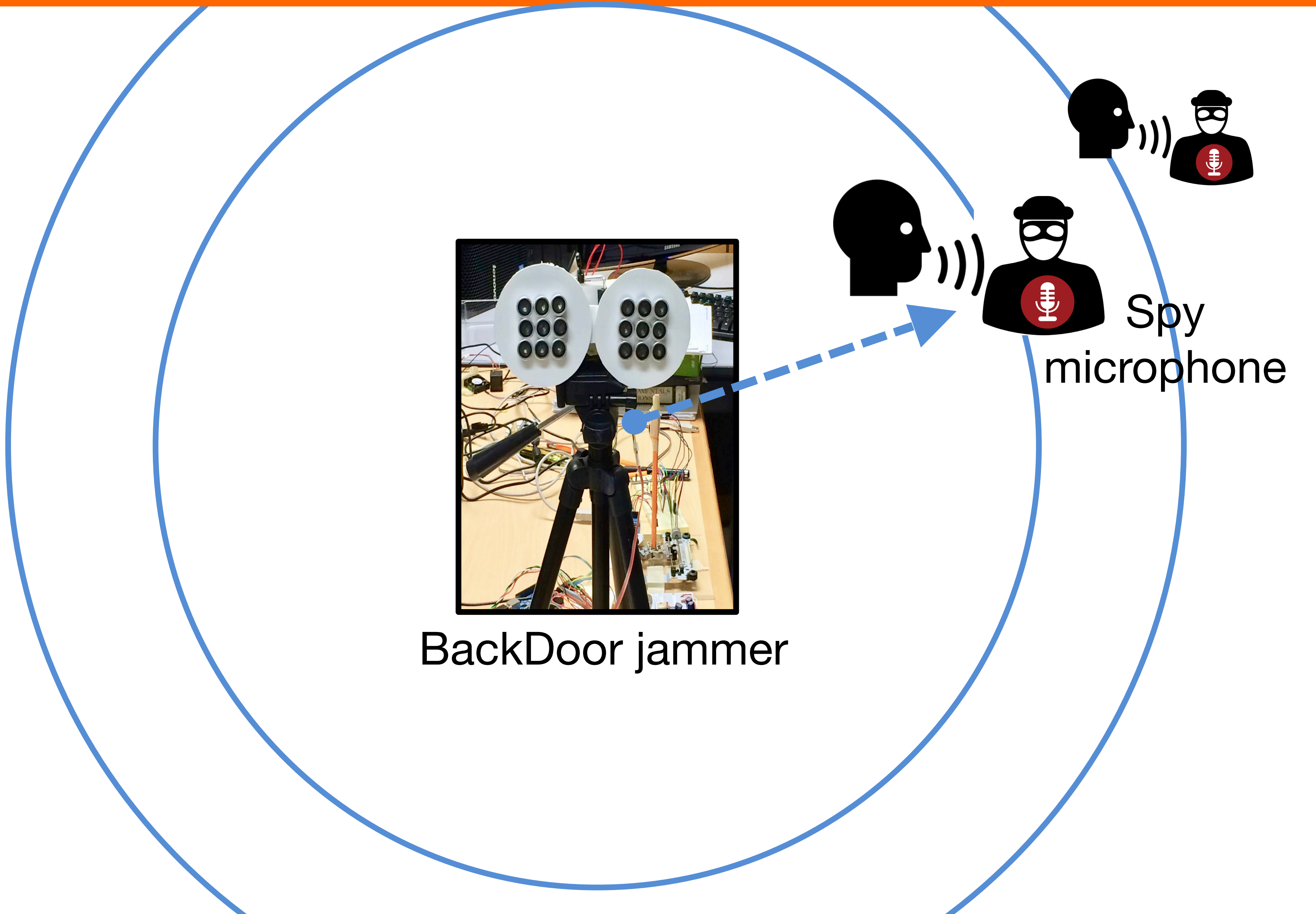
Jamming performance



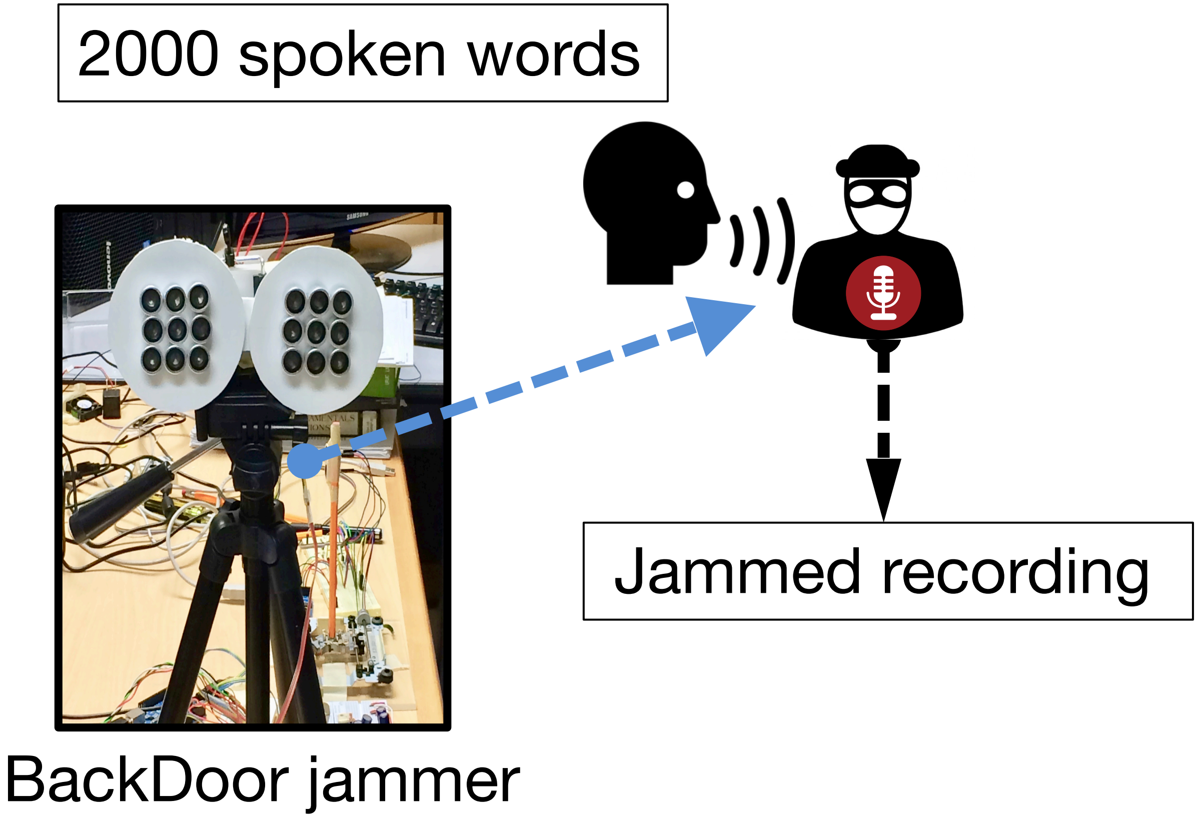
Jamming performance



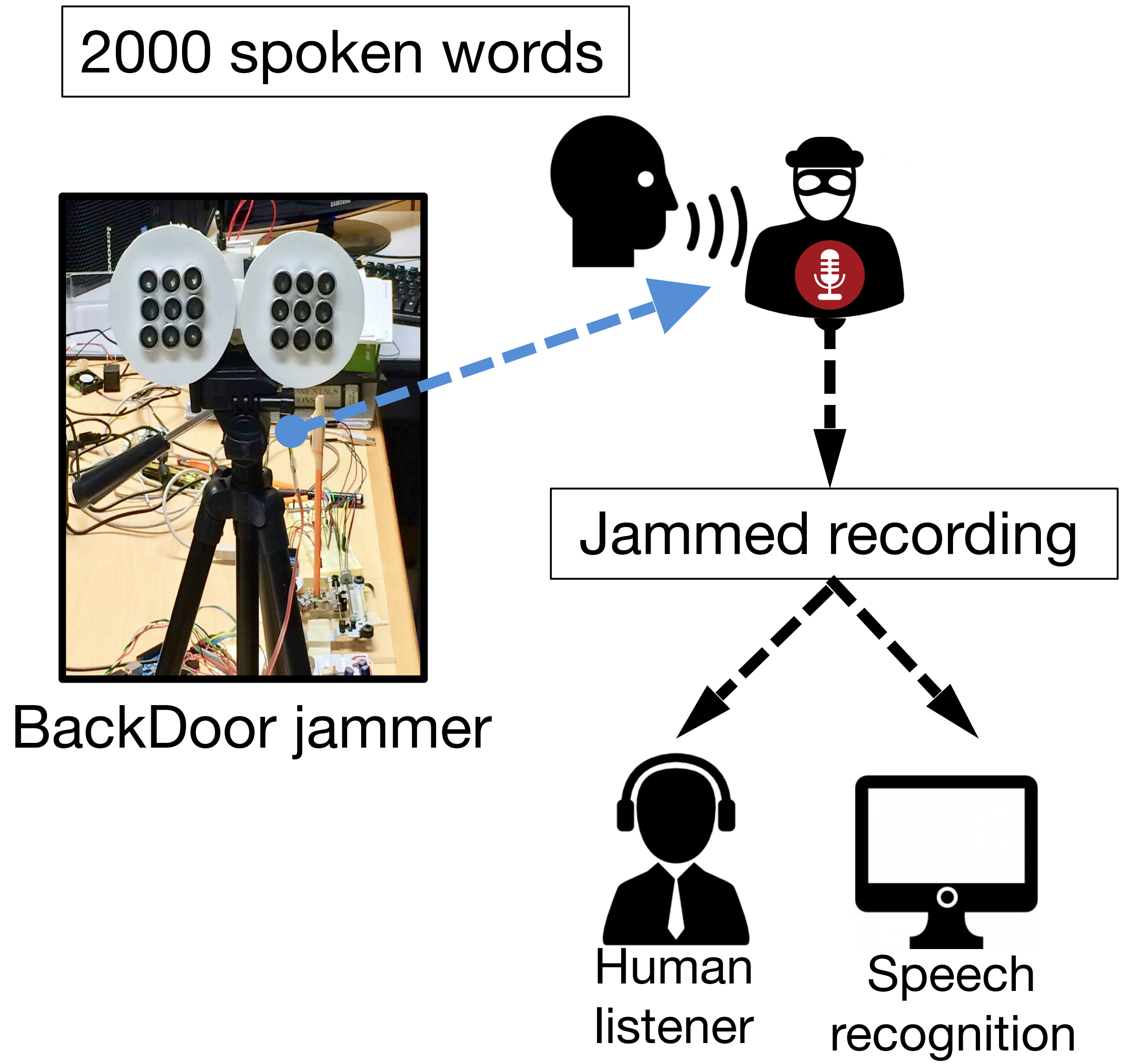
Jamming performance



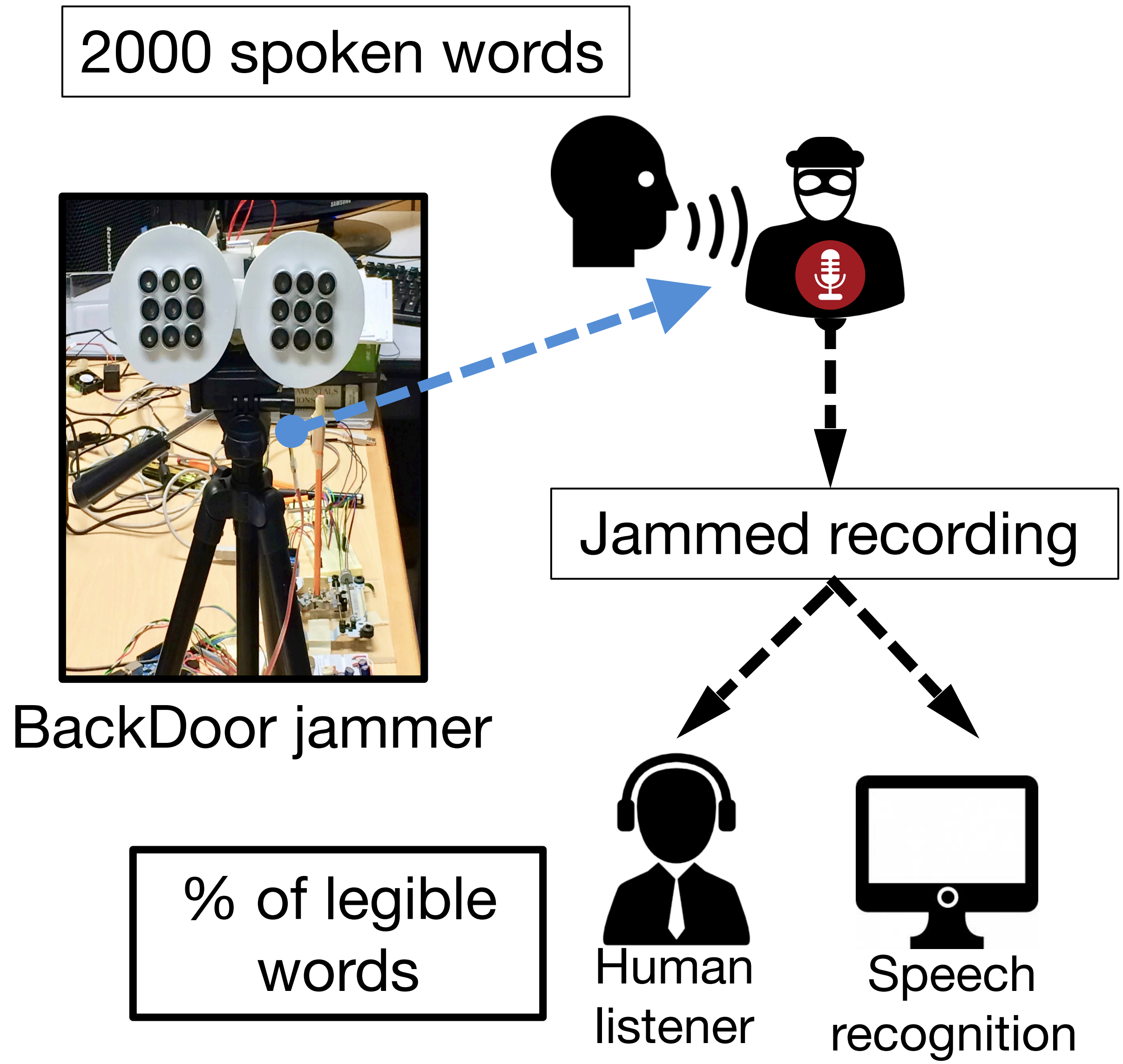
Jamming performance



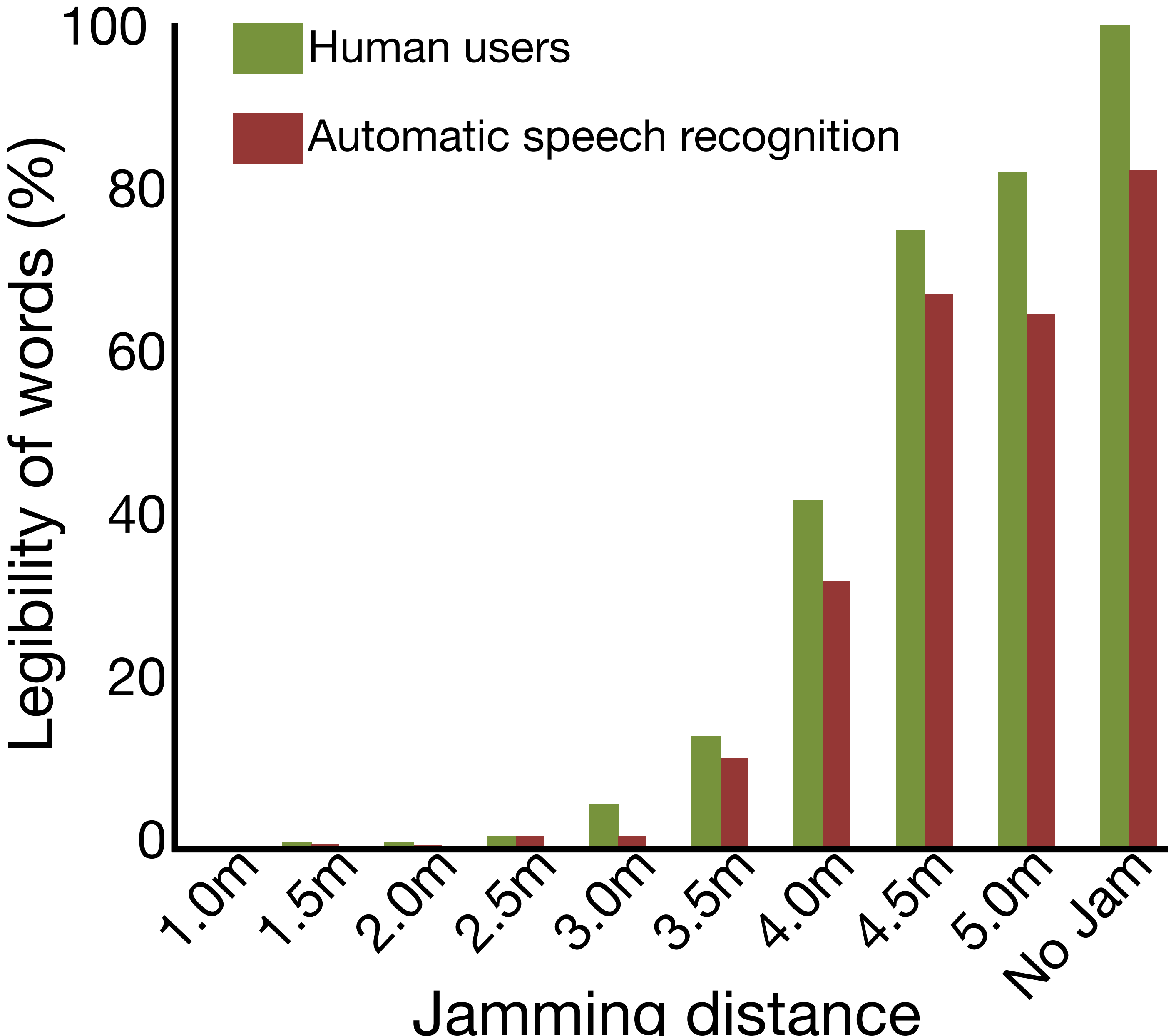
Jamming performance



Jamming performance



Jamming performance



How would you design a system to secure against this attack?

UEC TOKYO

M | CSE COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

LIGHT
COMMANDS

Summary

- IoT Security: both digital and analog
- “Sensor” security & attacks:
  - Mobile acoustic attacks (inaudible voice commands)
  - Analog Sensor attacks (on MEMS accelerometers)
  - Drone Security (Spoofing GPS)
  - Medical Security (Hacking Pacemakers)
- Modulation schemes
  - AM
  - FM
  - Inter-modulation
- Fundamentals have implications beyond IoT (e.g., Cuban “acoustic attack”)

MUTE: Bringing IoT to Noise Cancellation

Sheng Shen, Nirupam Roy, Junfeng Guan, Haitham Hassanieh, Romit Roy Choudhury
University of Illinois at Urbana-Champaign

ACM SIGCOMM 2018