BackDoor: Making Microphones Hear Inaudible Sounds

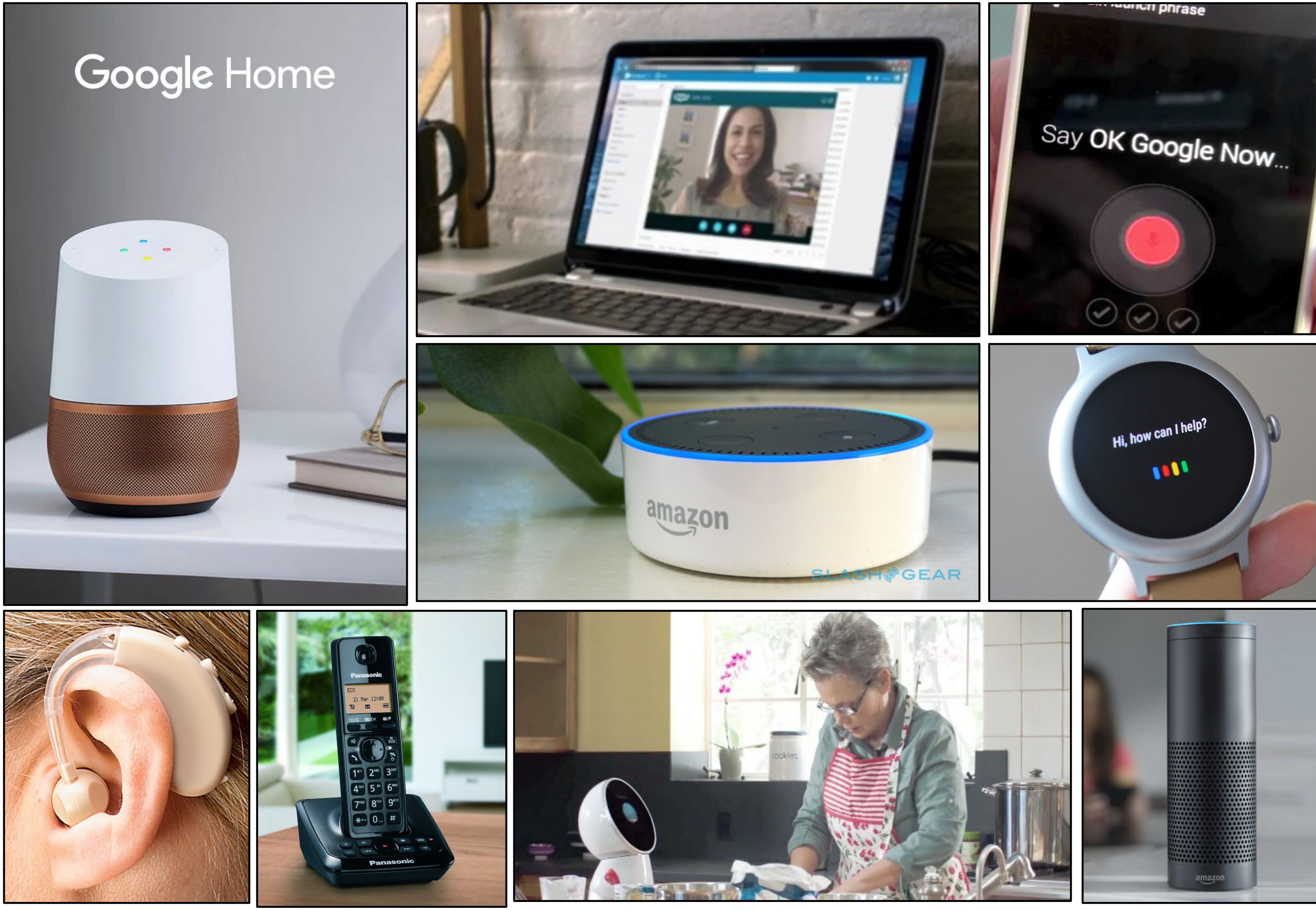

Nirupam Roy


Haitham Hassanieh

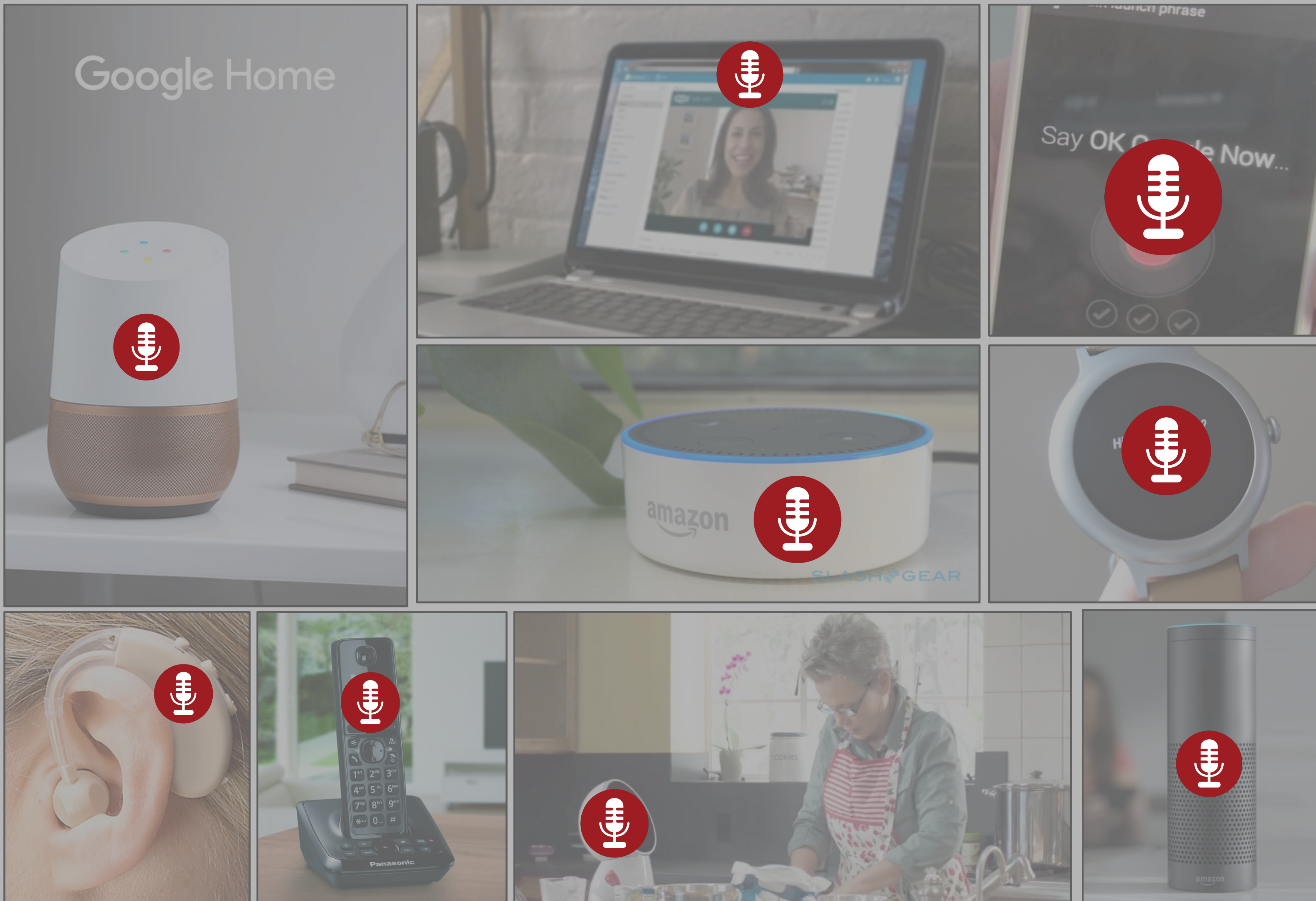

Romit Roy Choudhury

University of Illinois at Urbana-Champaign

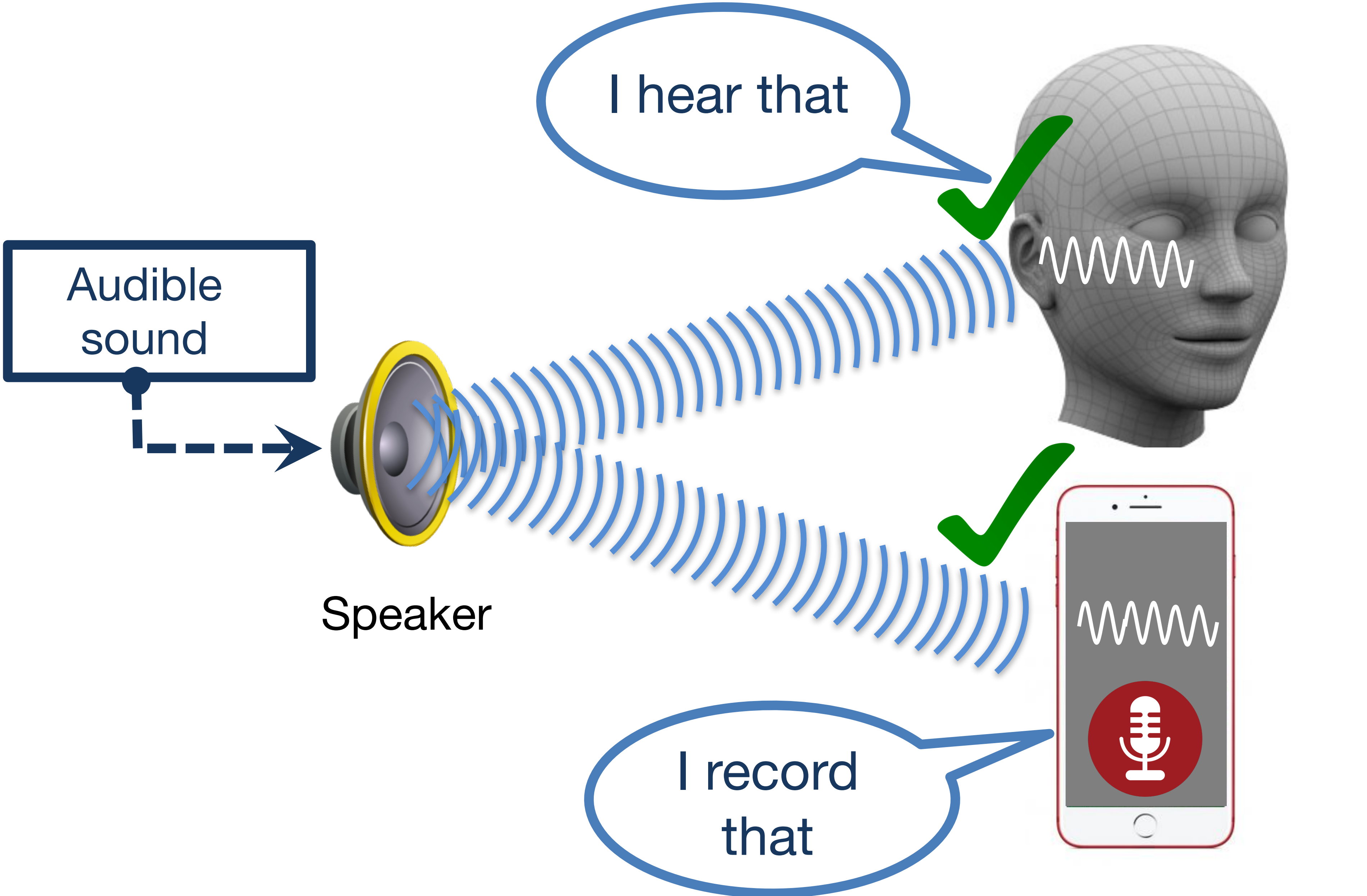
Microphones are everywhere



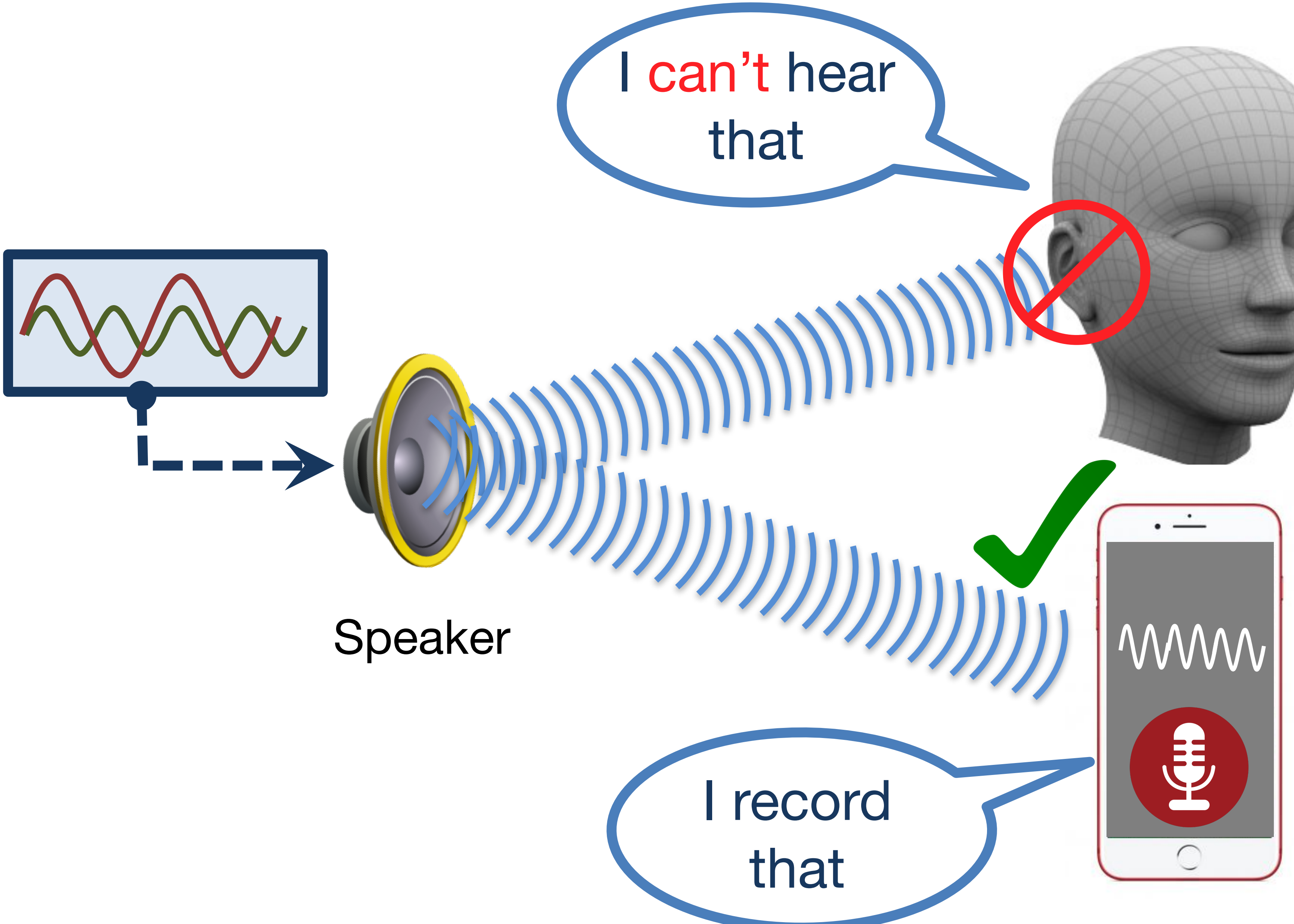
Microphones are everywhere



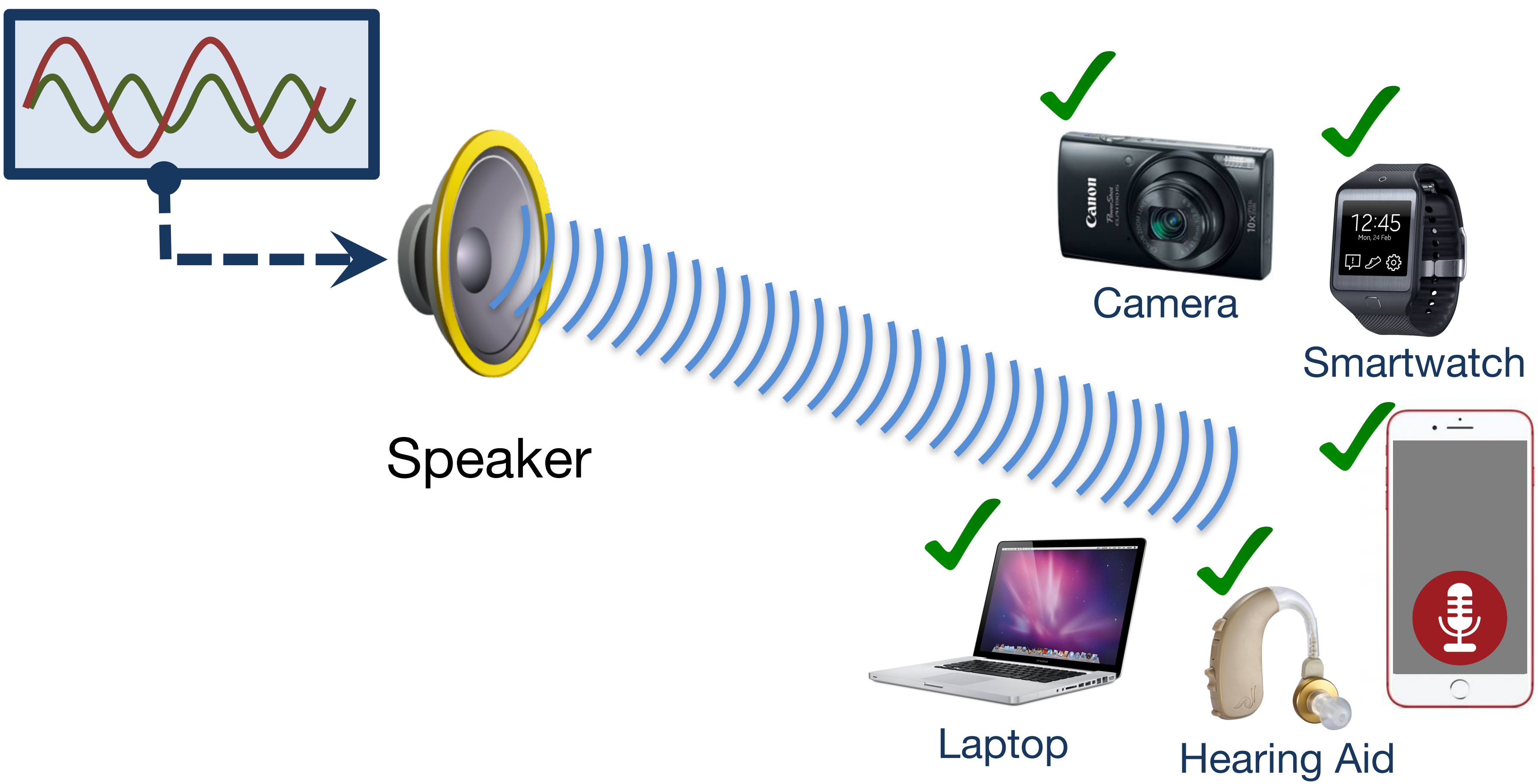
Microphones record audible sounds



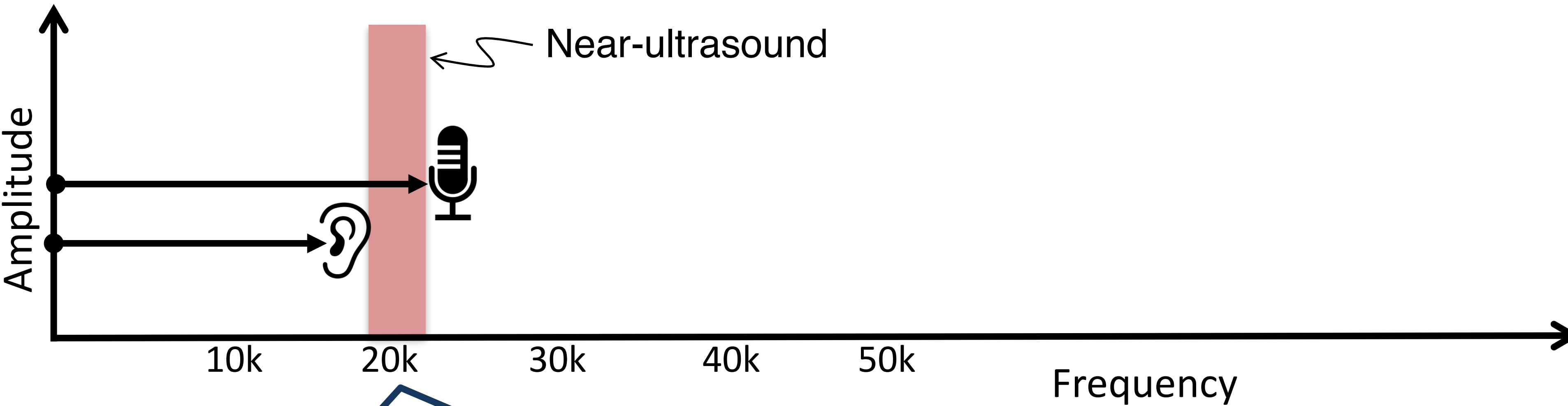
Inaudible, but recordable !



Works with unmodified devices



It's not "near-ultrasound"



chirp.io

Pseudo-ranging
SenSys'12

ApneaApp
MobiSys'15

DopLink
UbiComp'13

SoundWave
CHI'12

lisnr.com

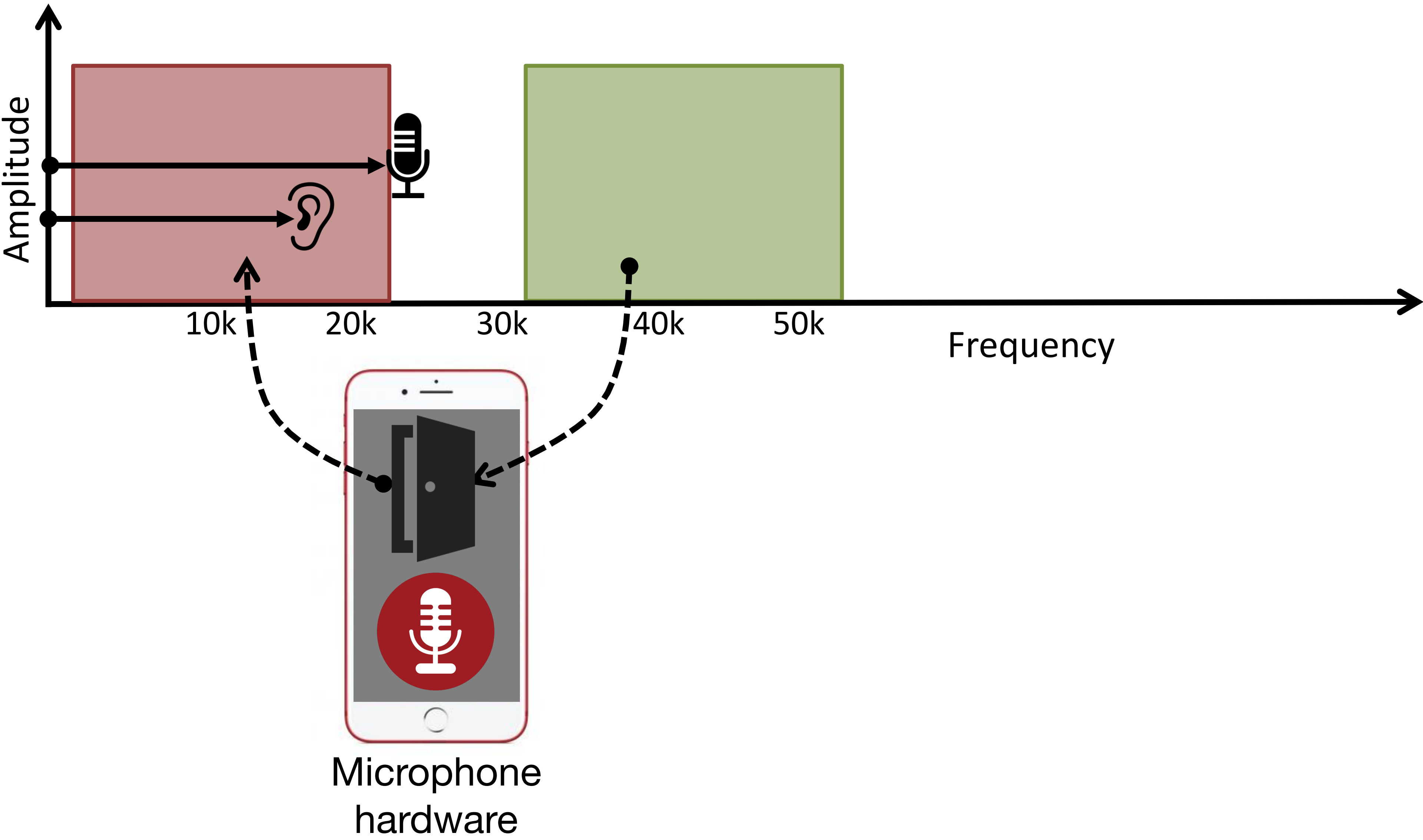
AAMouse
MobiSys'15

AirLink
UbiComp'14

Spartacus
MobiSys'13

Crowd-counting
SenSys'12

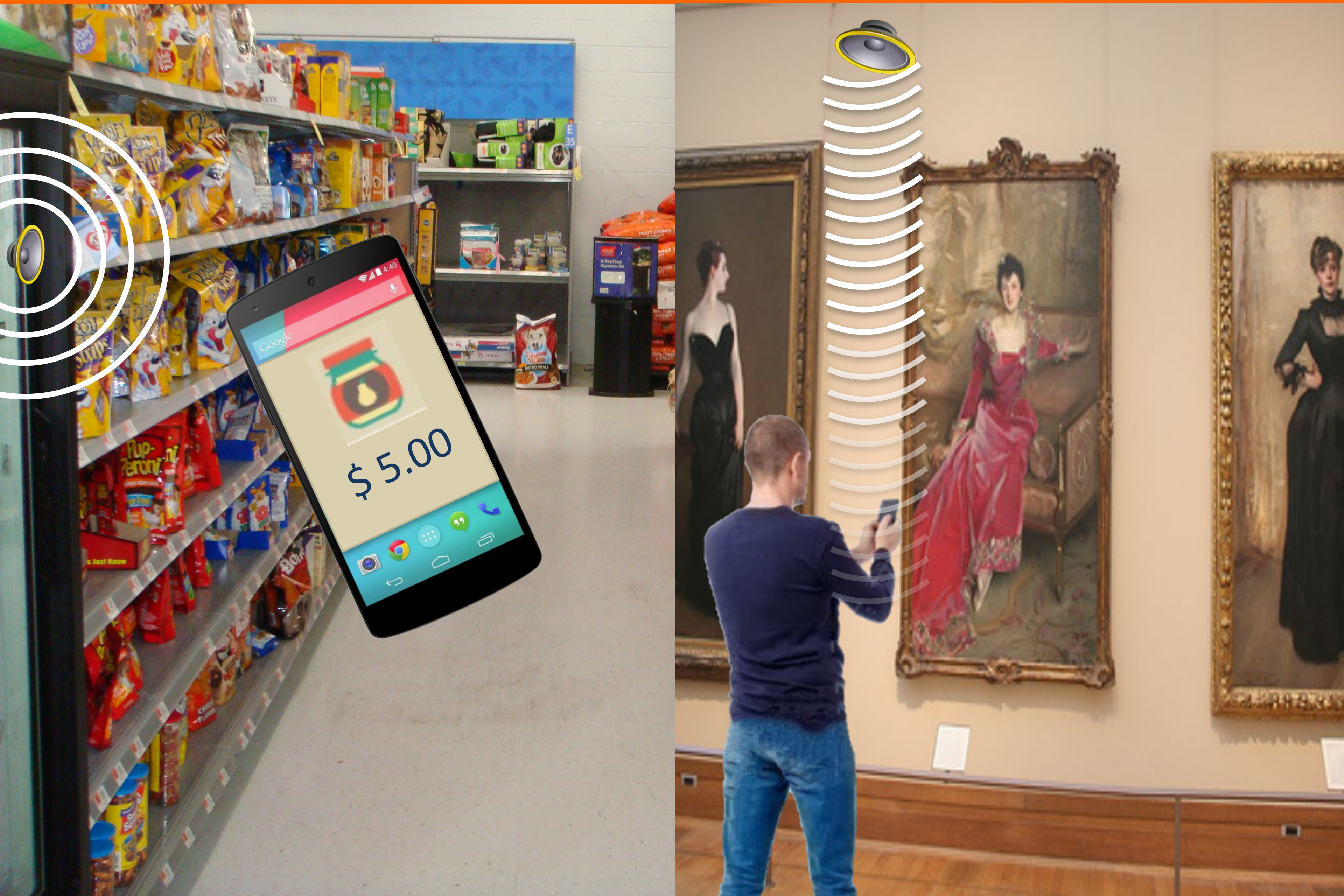
Exploiting fundamental nonlinearity



What can we do with it?

Application: Acoustic jammer

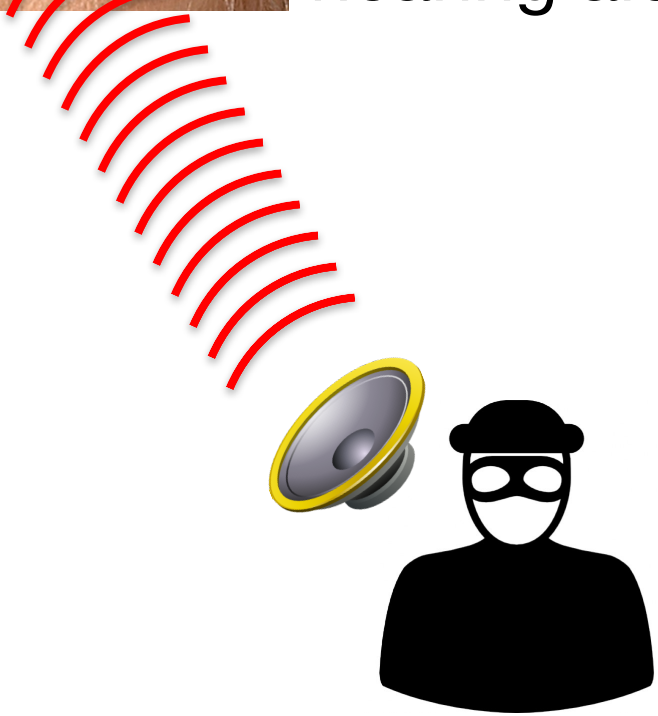
Application: Acoustic communication



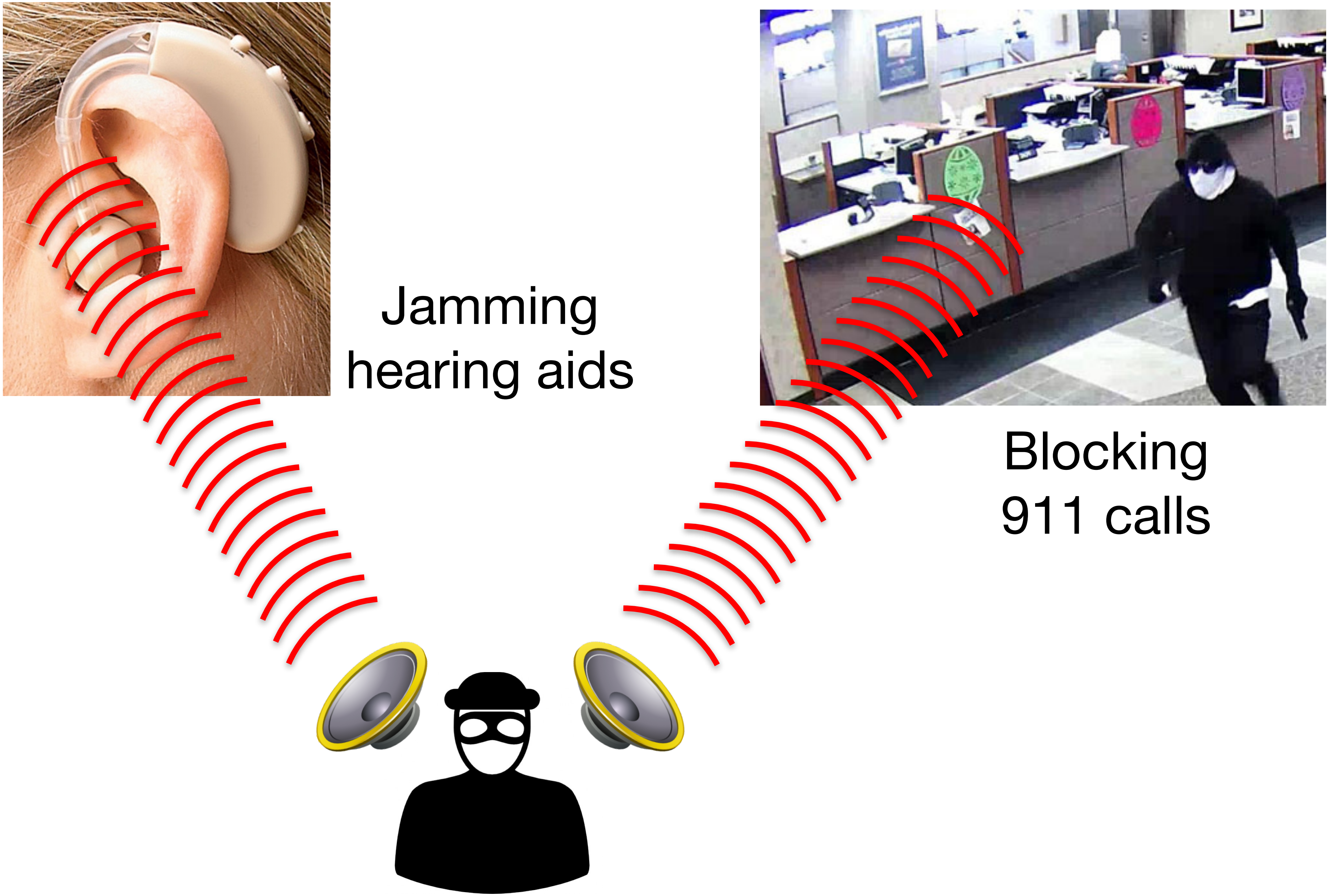
Threat: Acoustic DOS attack

Threat: Acoustic DOS attack

Jamming
hearing aids



Threat: Acoustic DOS attack



Talk outline

① Microphone Overview

② System Design

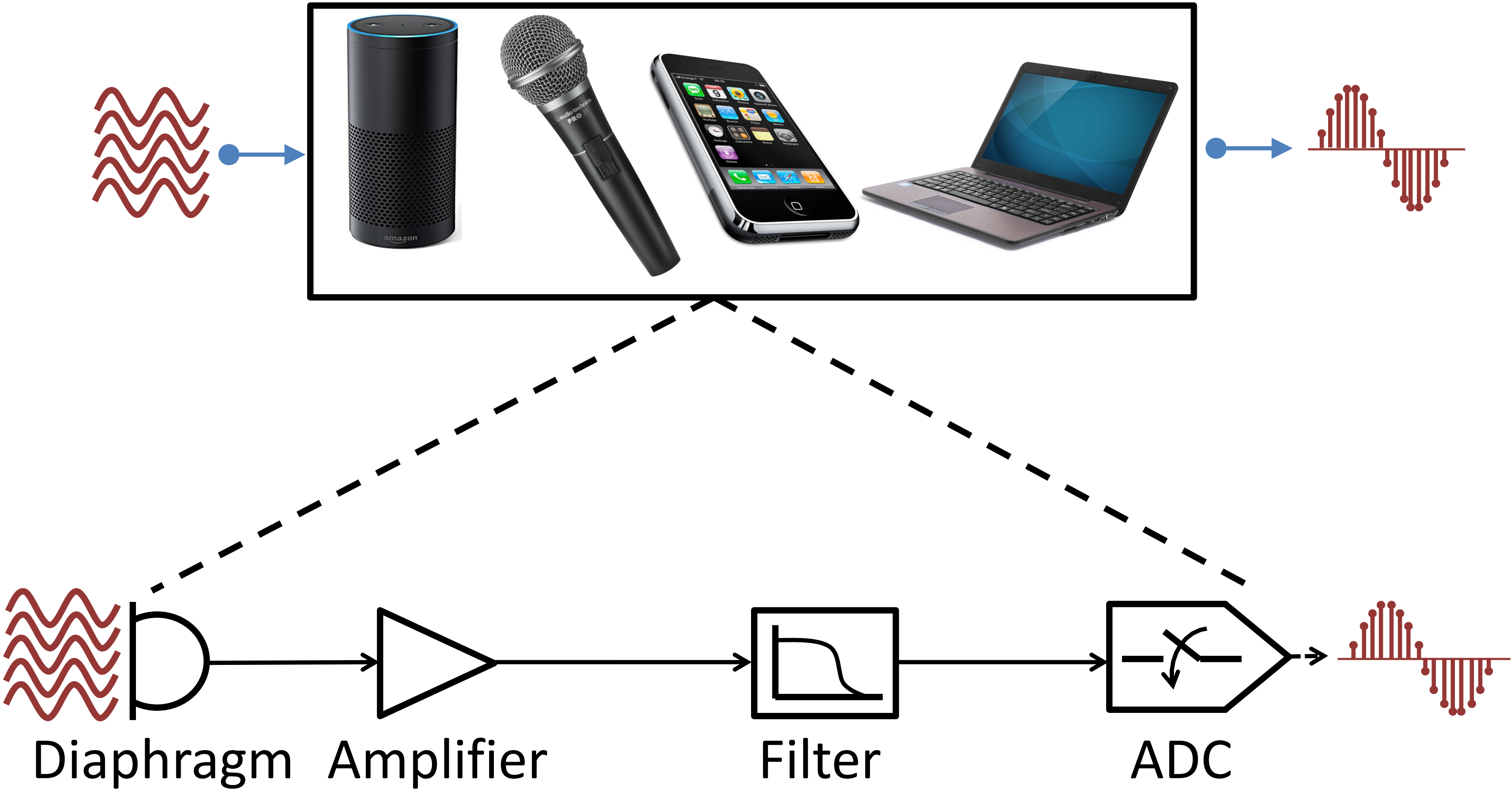
③ Challenges

④ Evaluation

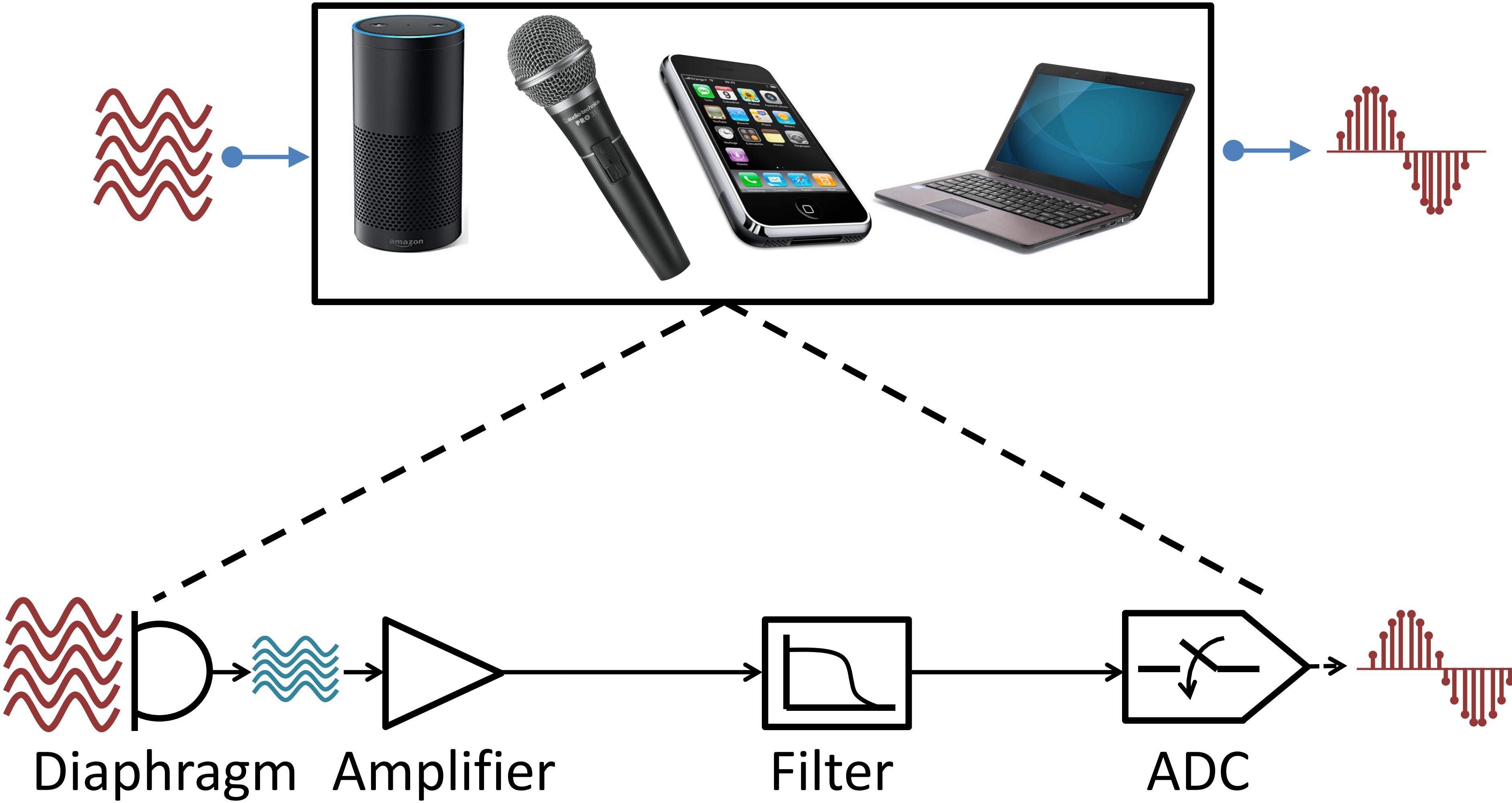
Talk outline

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

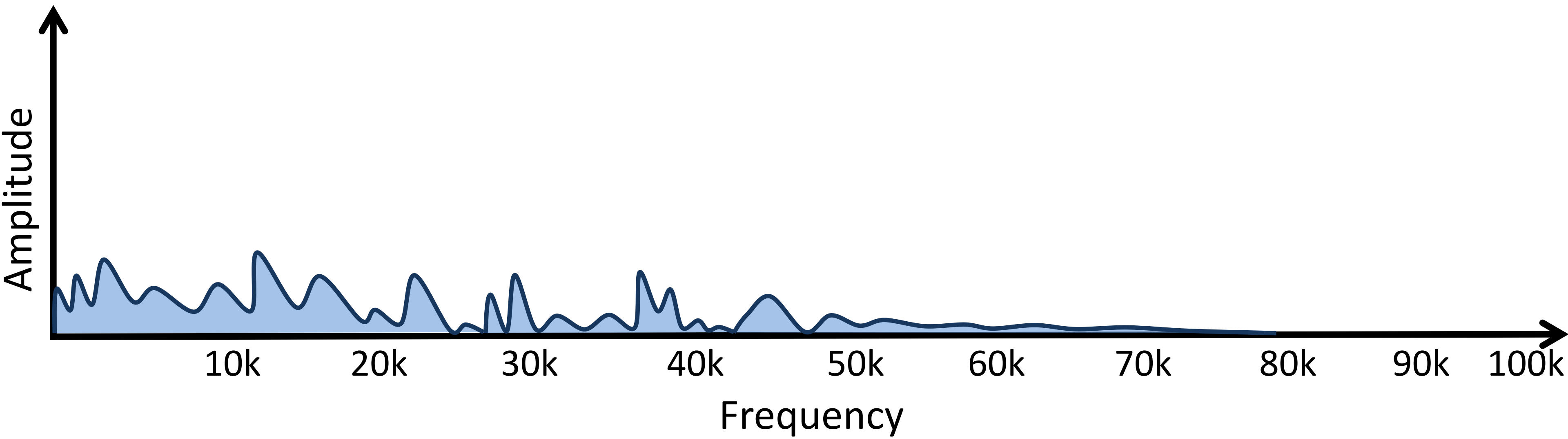
Microphone working principle

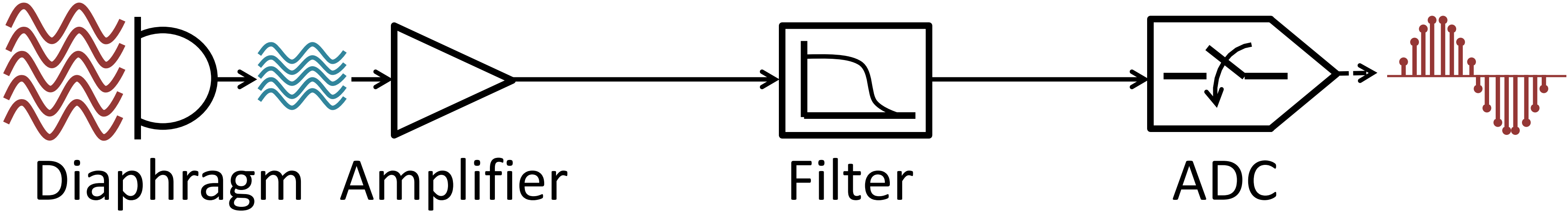


Microphone working principle

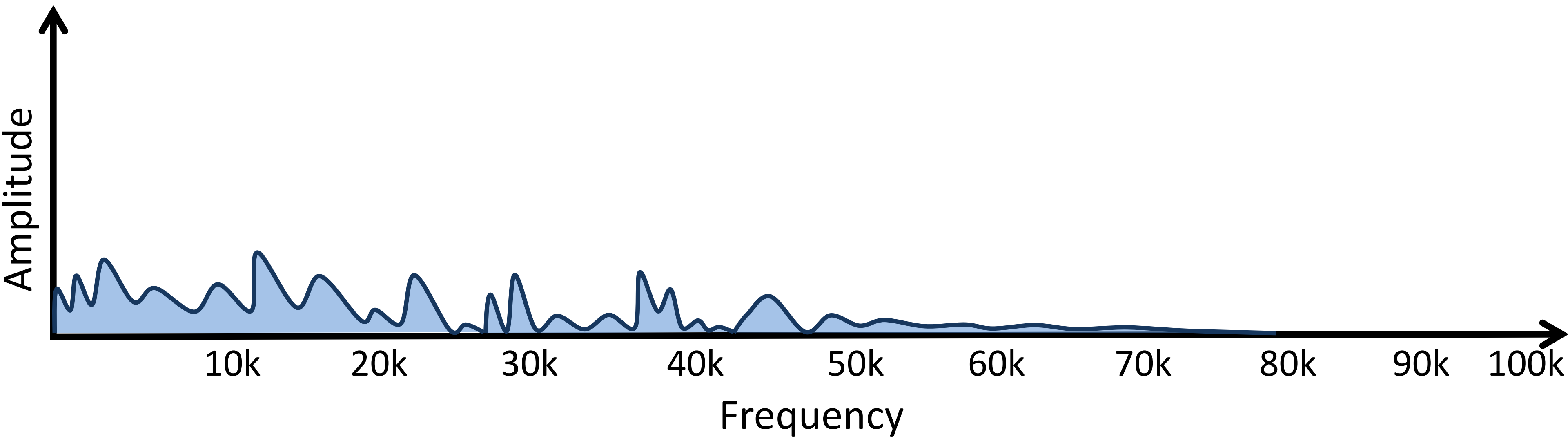


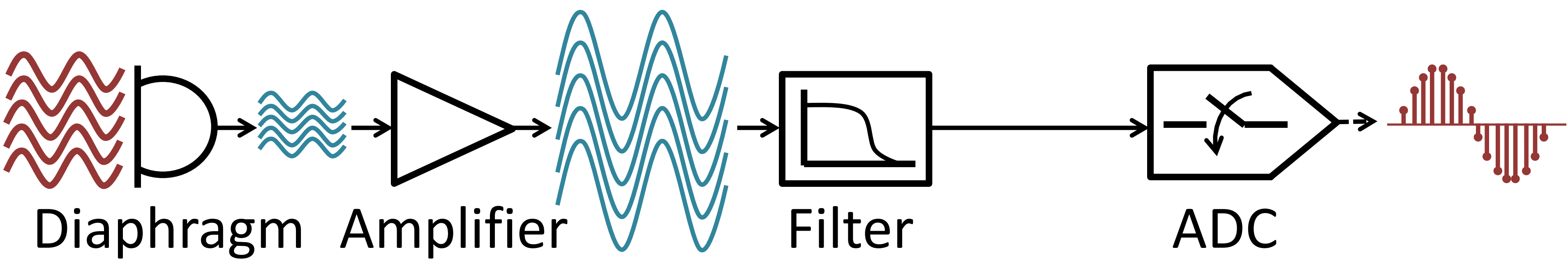
Microphone working principle



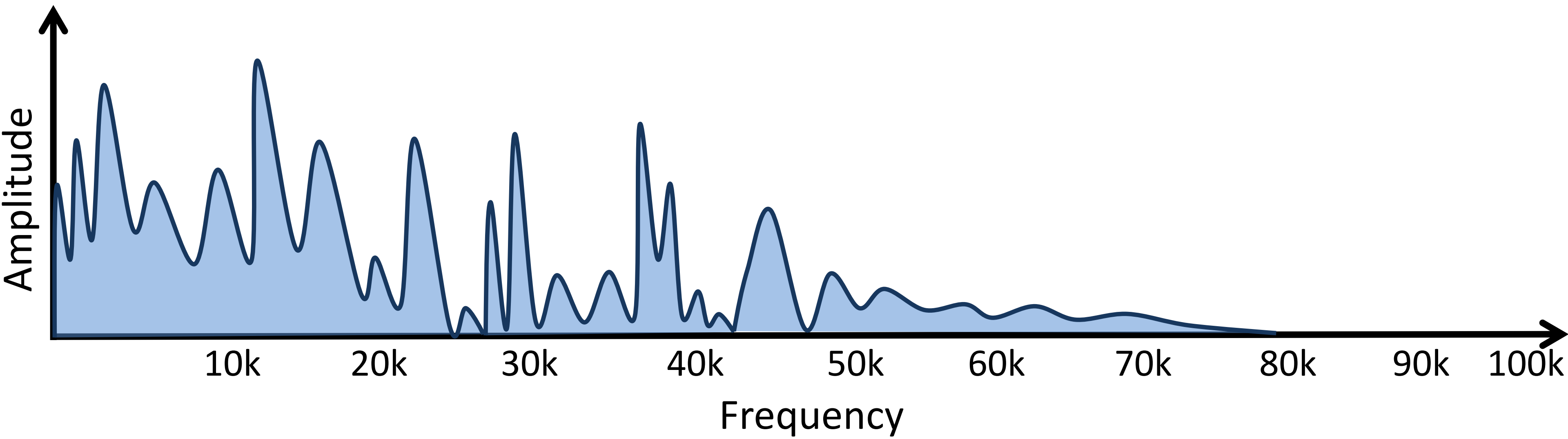


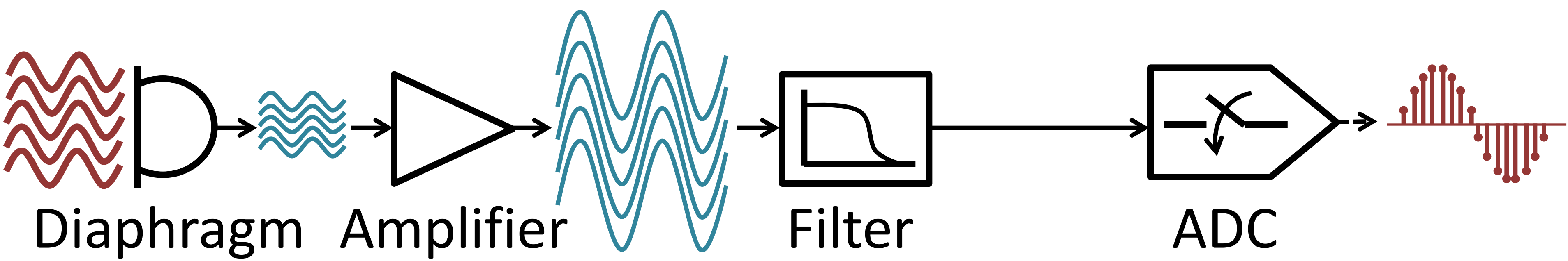
Microphone working principle



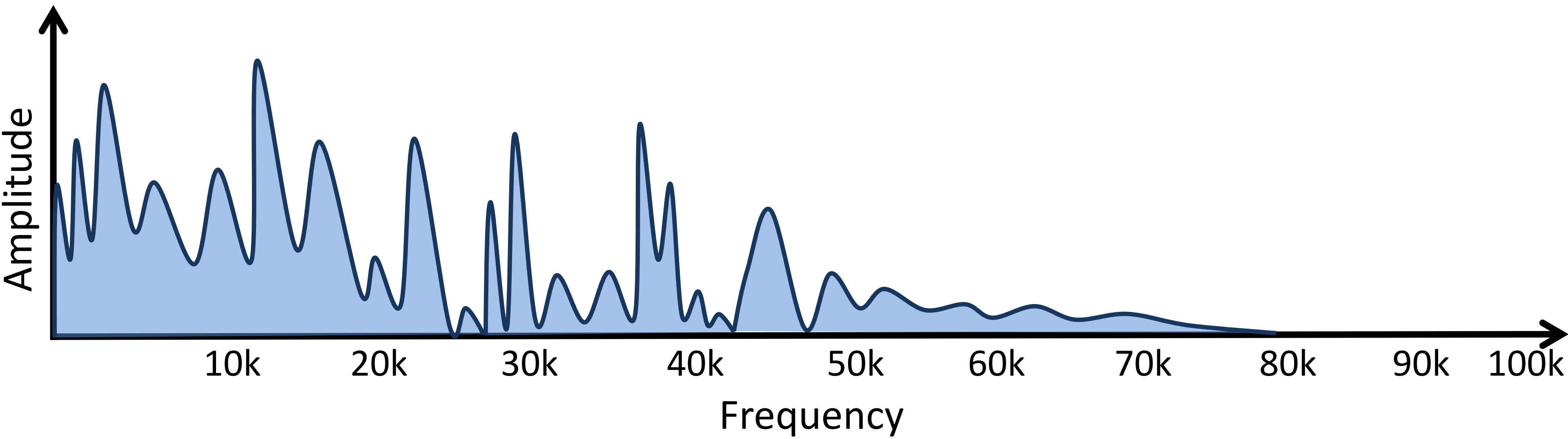


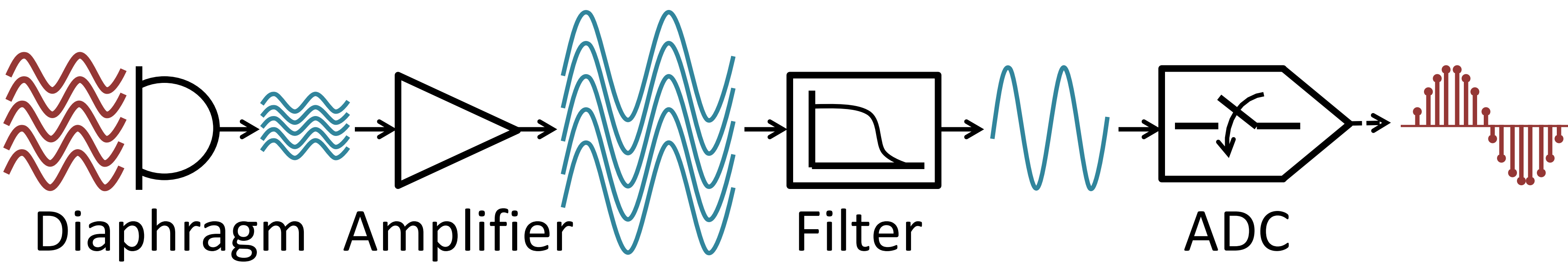
Microphone working principle



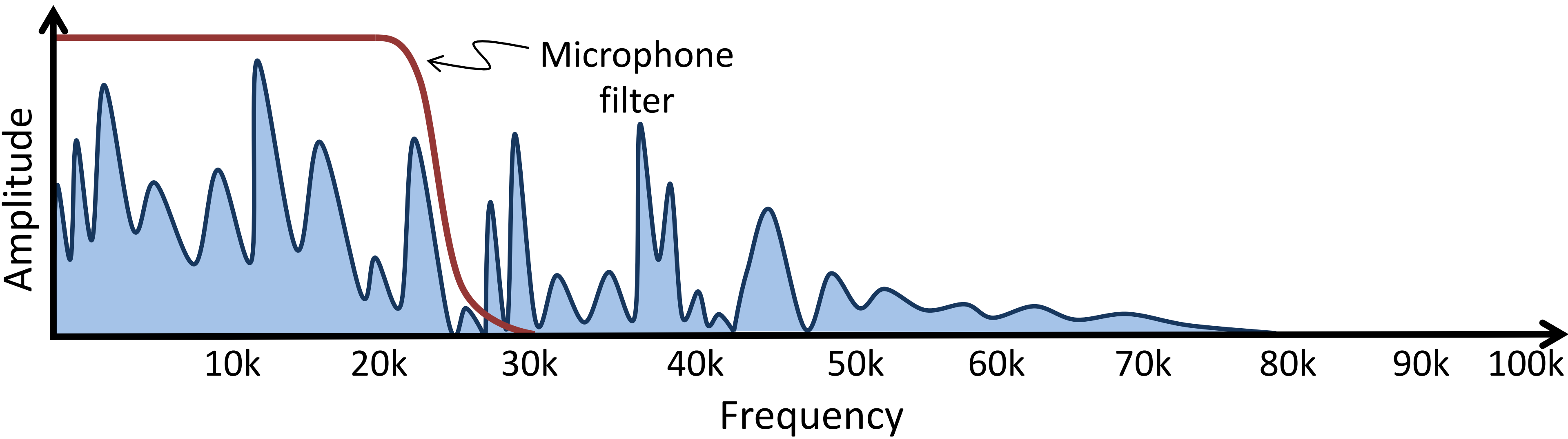


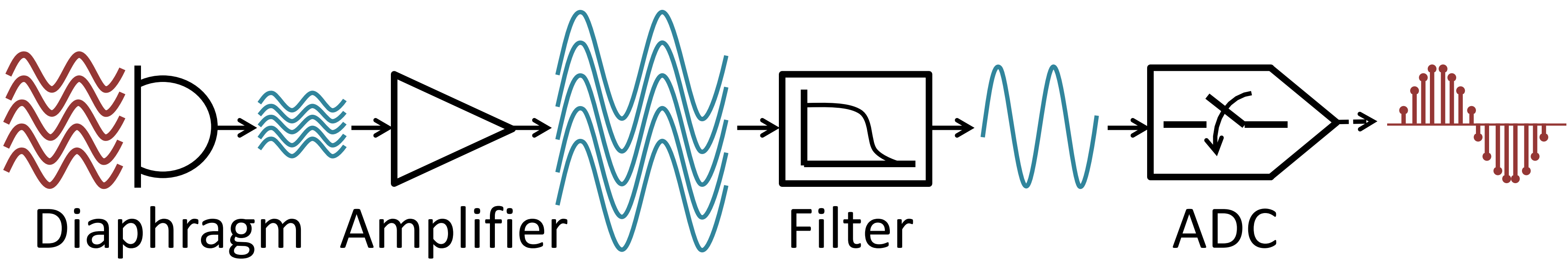
Microphone working principle



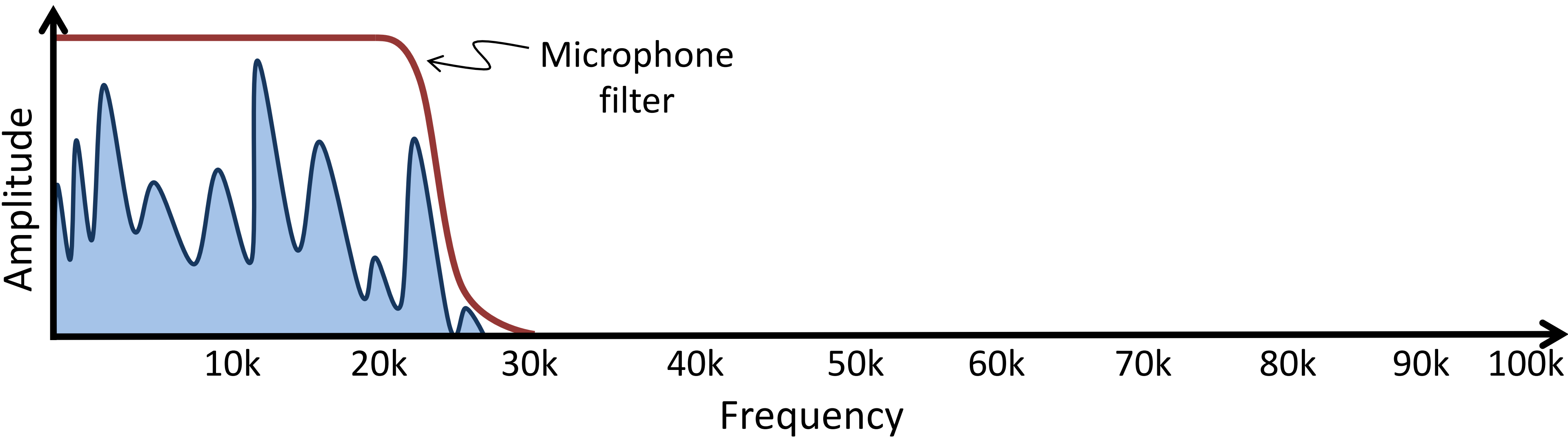


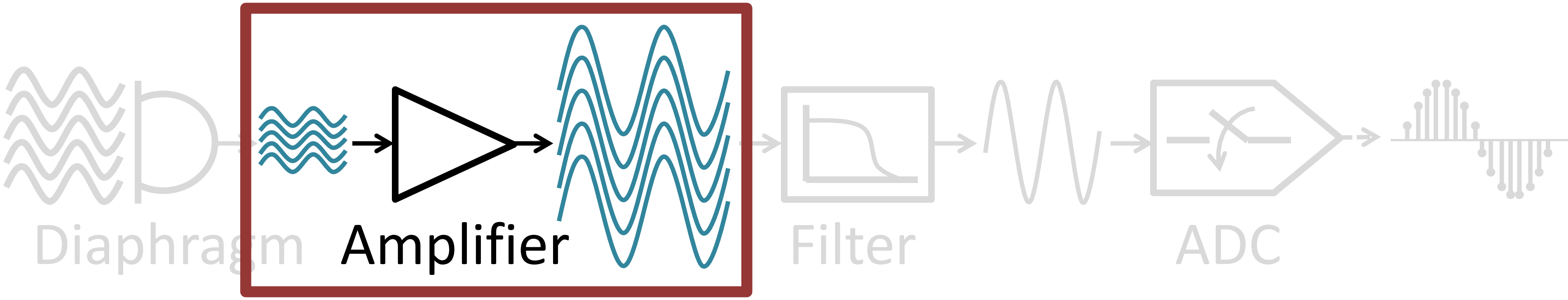
Microphone working principle



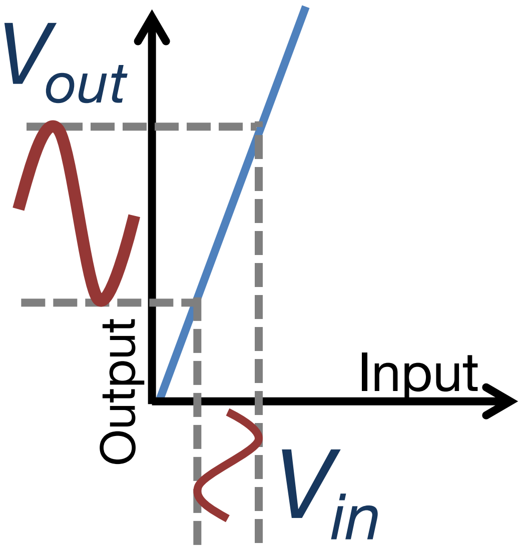


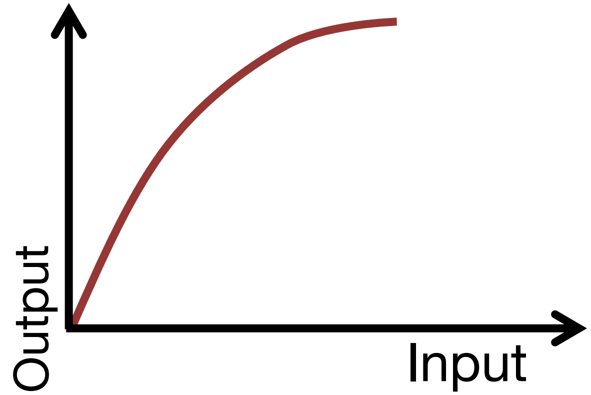
Microphone working principle





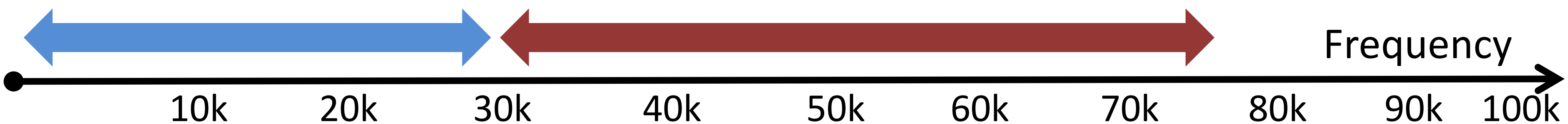
Microphone working principle

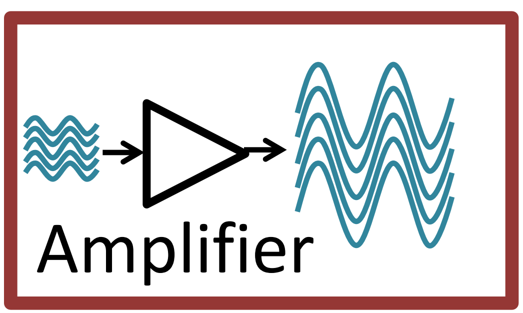




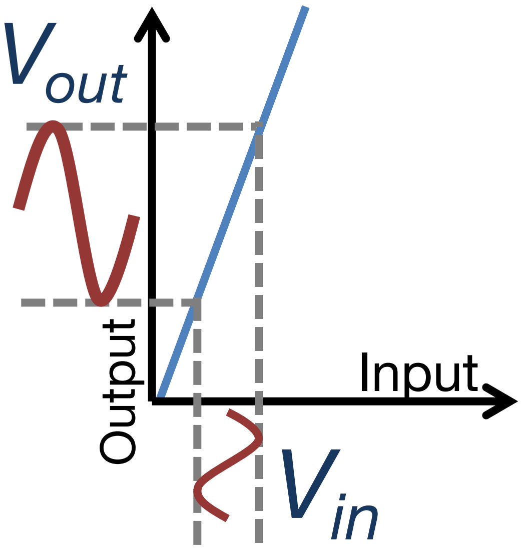
$$V_{out} = a_1 V_{in}$$

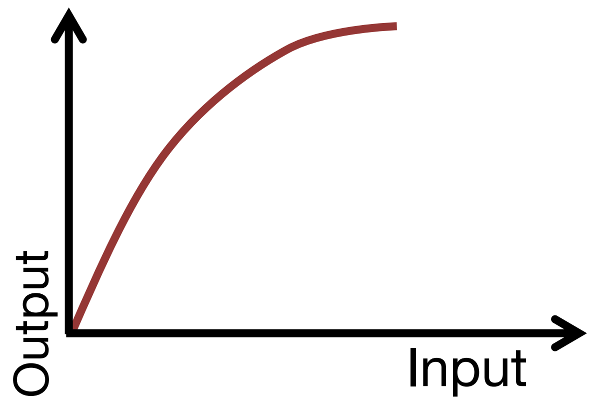
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \dots$$





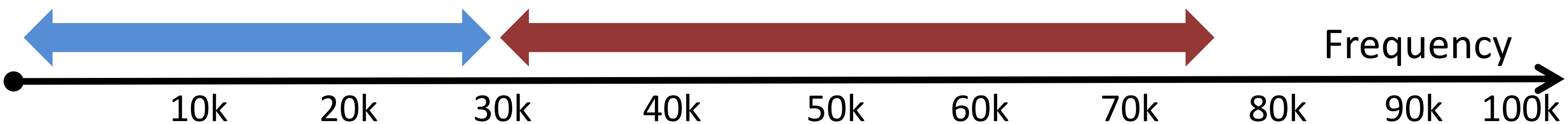
Microphone working principle

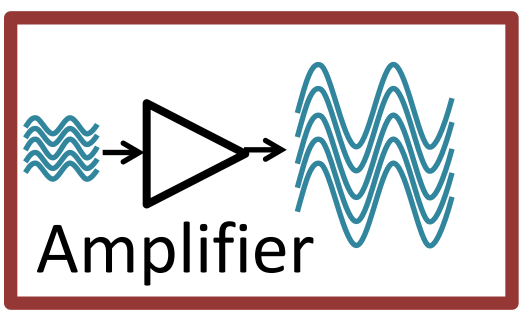




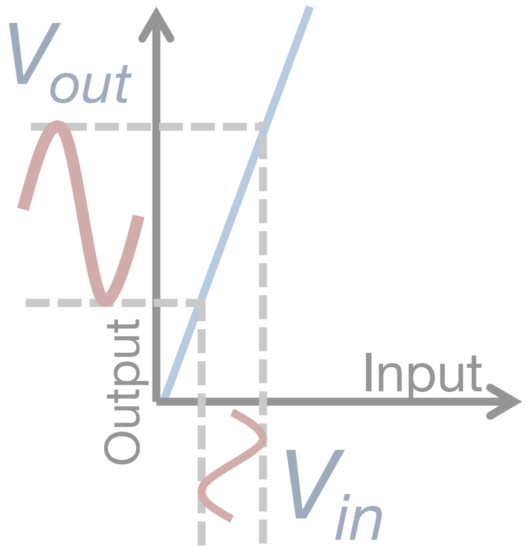
$$V_{out} = a_1 V_{in}$$

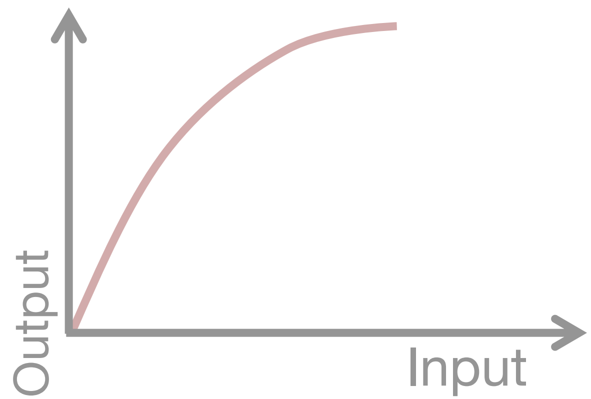
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$





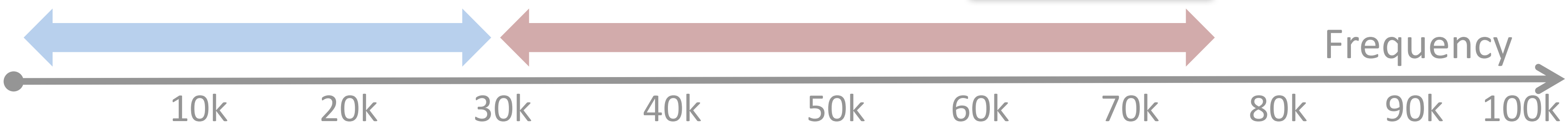
Microphone working principle

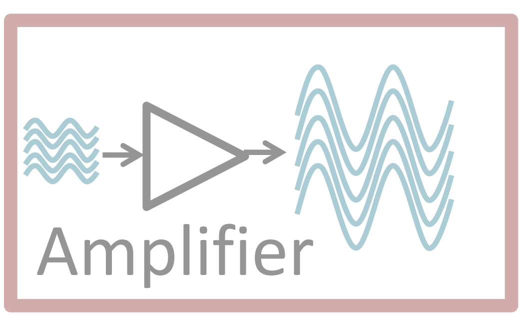




$$V_{out} = a_1 V_{in}$$

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

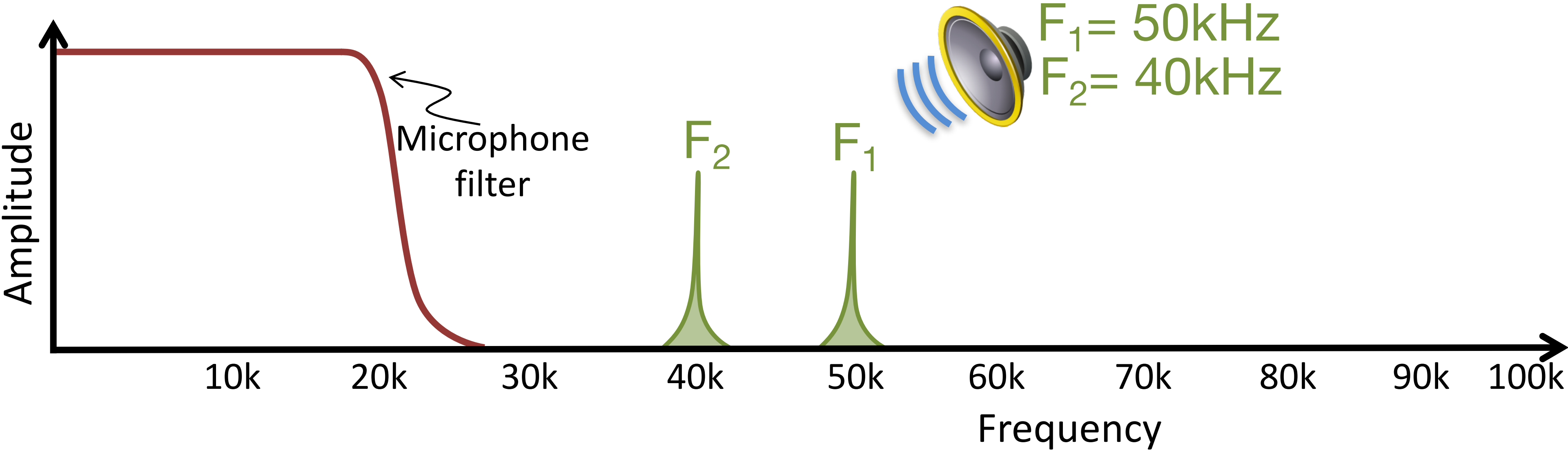




Talk outline

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

Exploiting amplifier non-linearity



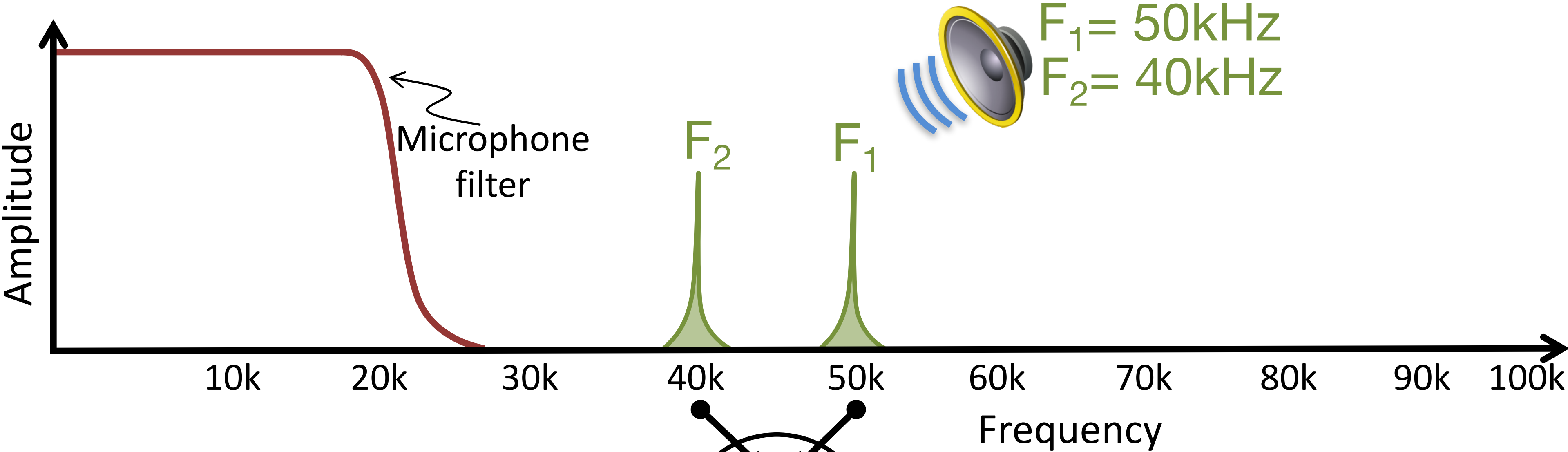
$$S_{out} = A_1(S_1 + S_2) + A_2(S_1 + S_2)^2$$

$$= A_1\{Sin(\omega_1 t) + Sin(\omega_2 t)\} \; + A_2\{Sin^2(\omega_1 t) +$$

$$Sin^2(\omega_2 t) + 2Sin(\omega_1 t)Sin(\omega_2 t)\}$$

where $\omega_1 = 2\pi 40$ and $\omega_2 = 2\pi 50$.

Exploiting amplifier non-linearity

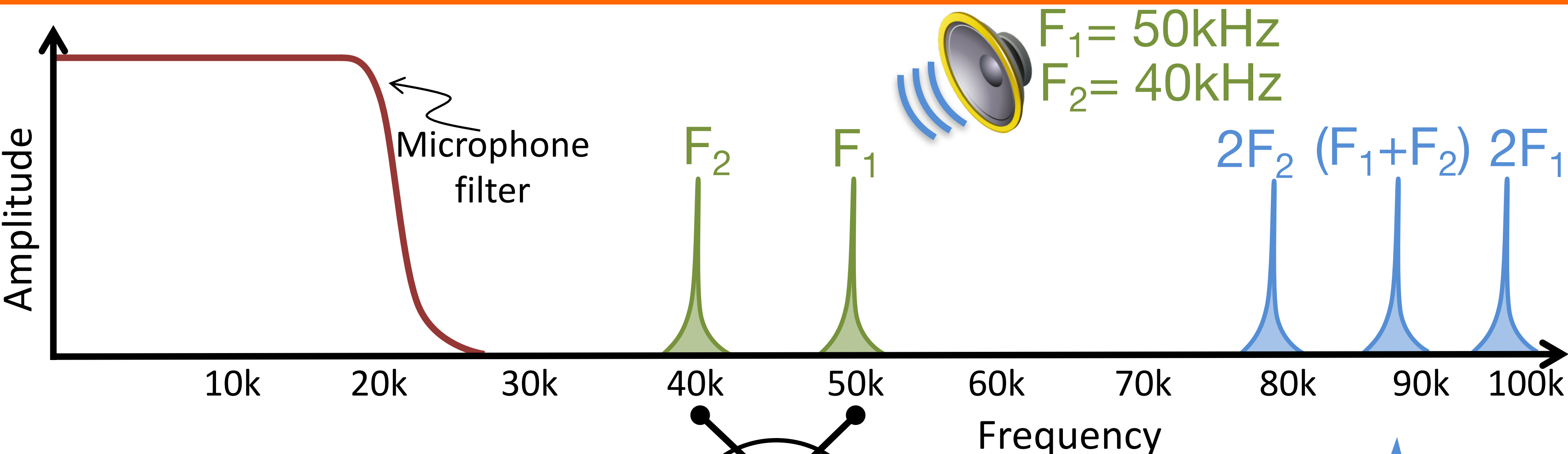


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

$$A_2(S_1+S_2)^2 = 1 - \frac{1}{2}Cos(2\omega_1 t) - \frac{1}{2}Cos(2\omega_2 t) + Cos((\omega_1 - \omega_2)t) - Cos((\omega_1 + \omega_2)t)$$

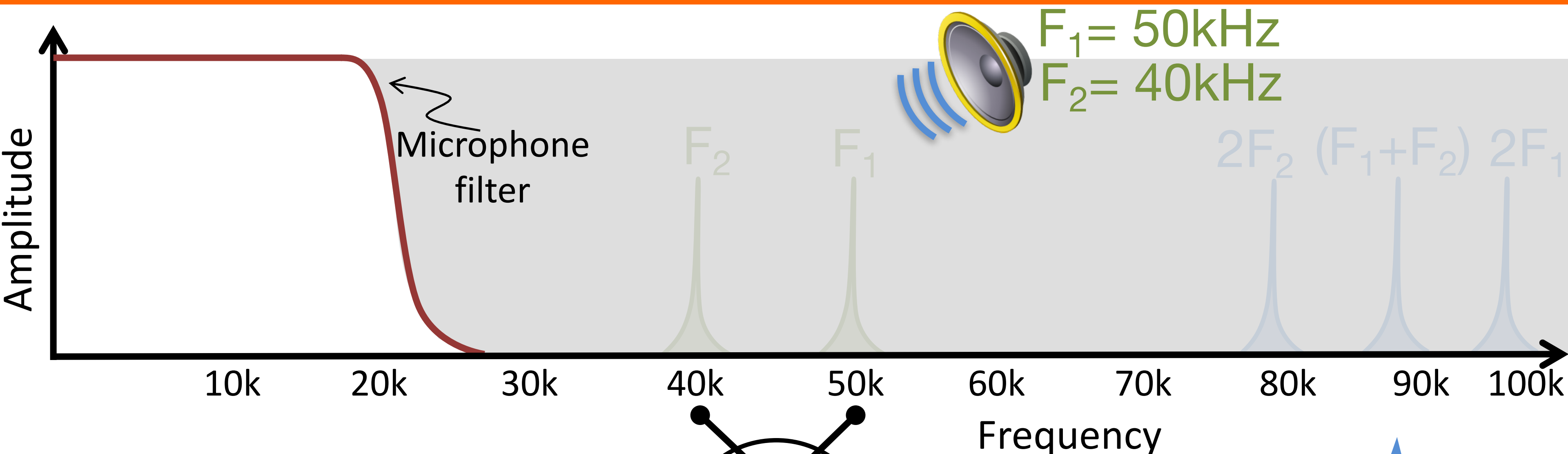
Exploiting amplifier non-linearity



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

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

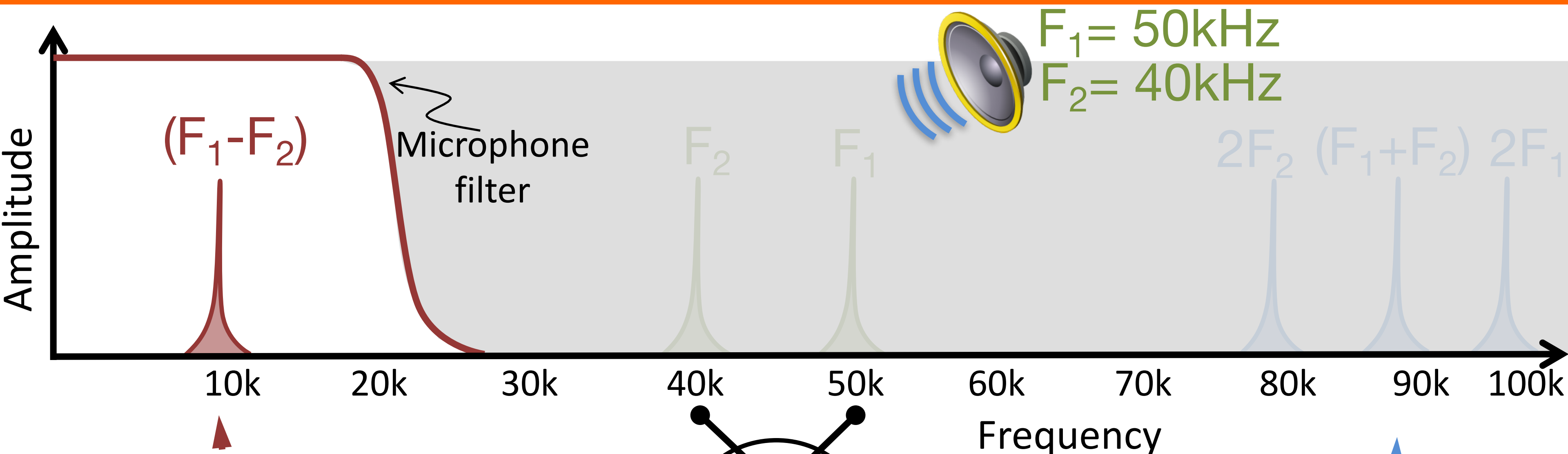
Exploiting amplifier non-linearity



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

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

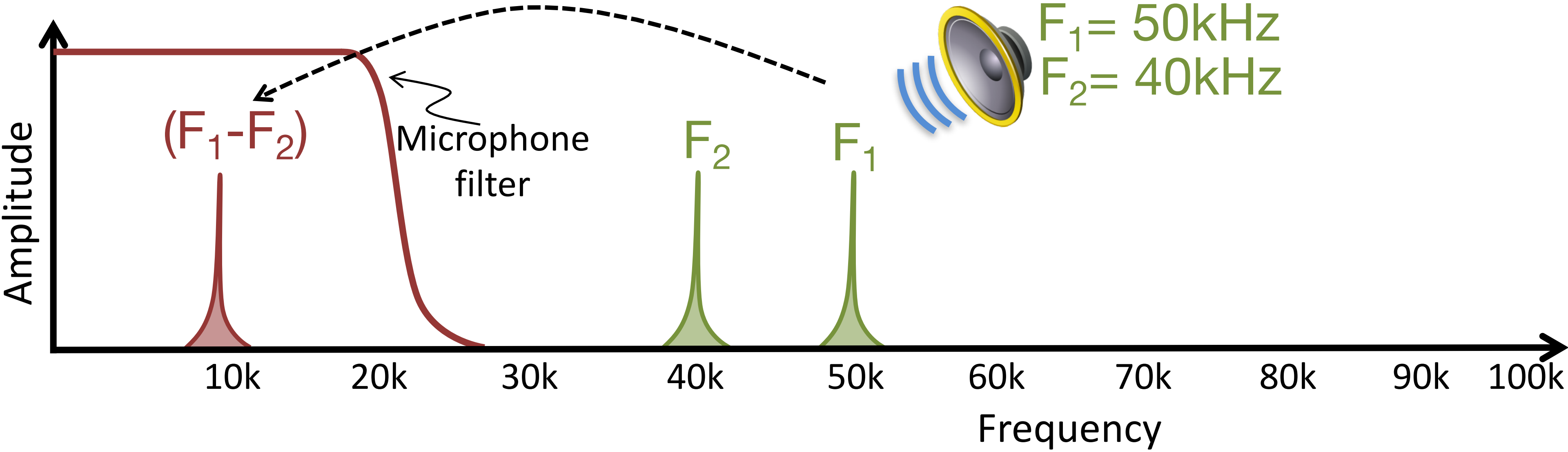
Exploiting amplifier non-linearity



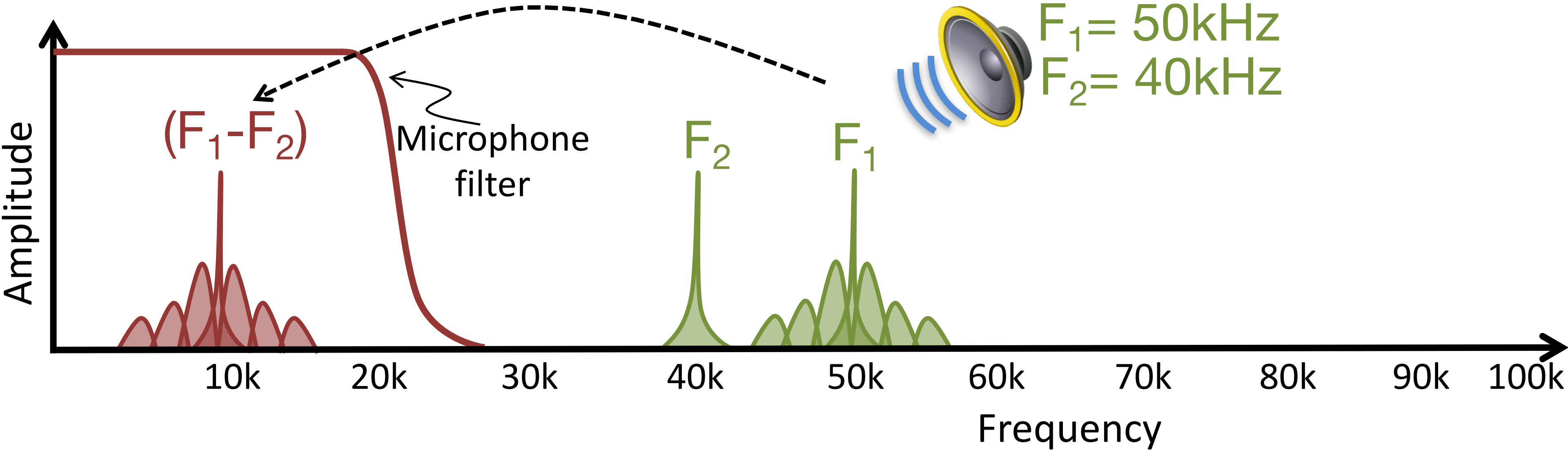
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

Exploiting amplifier non-linearity



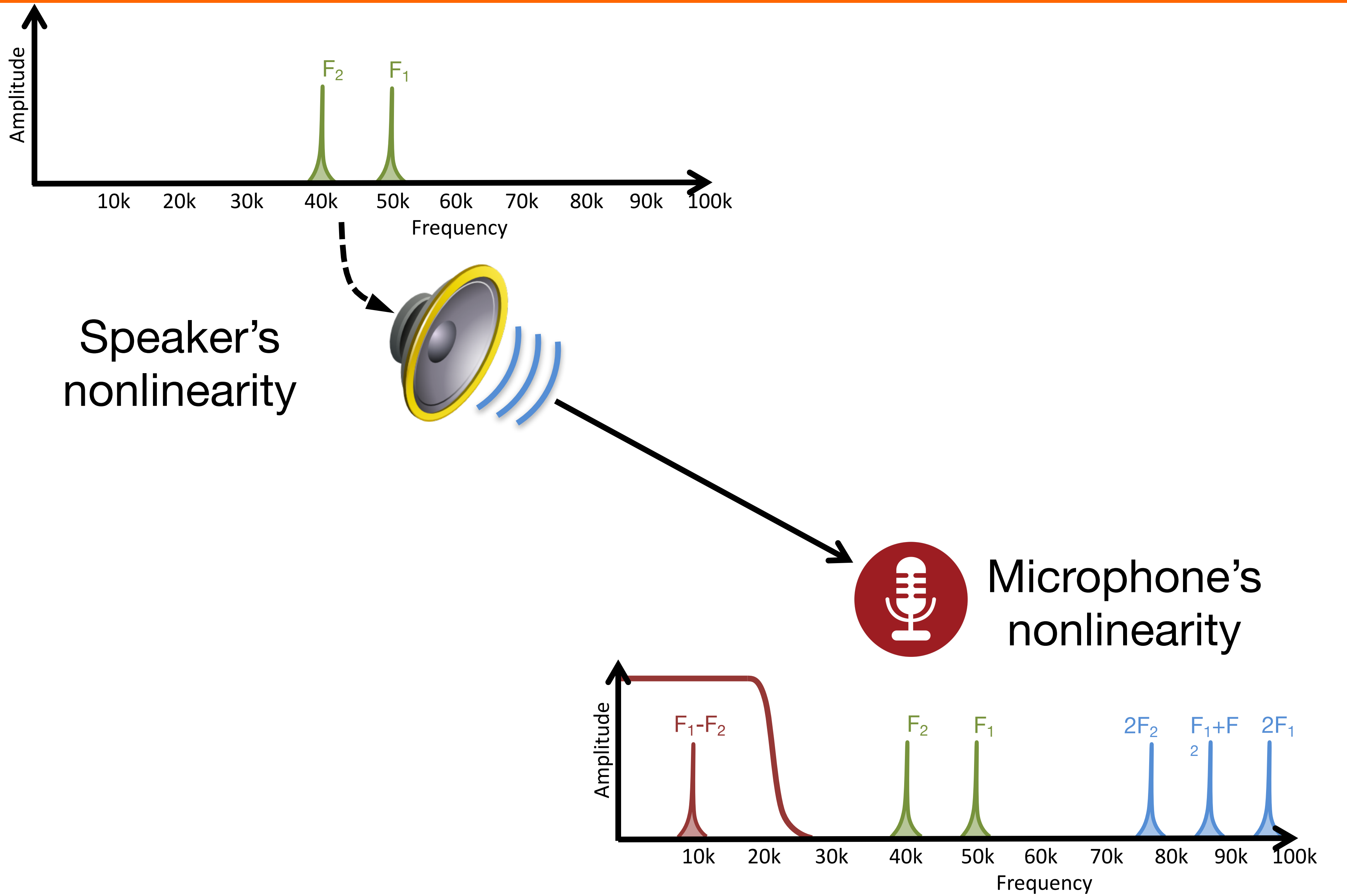
Exploiting amplifier non-linearity



Talk outline

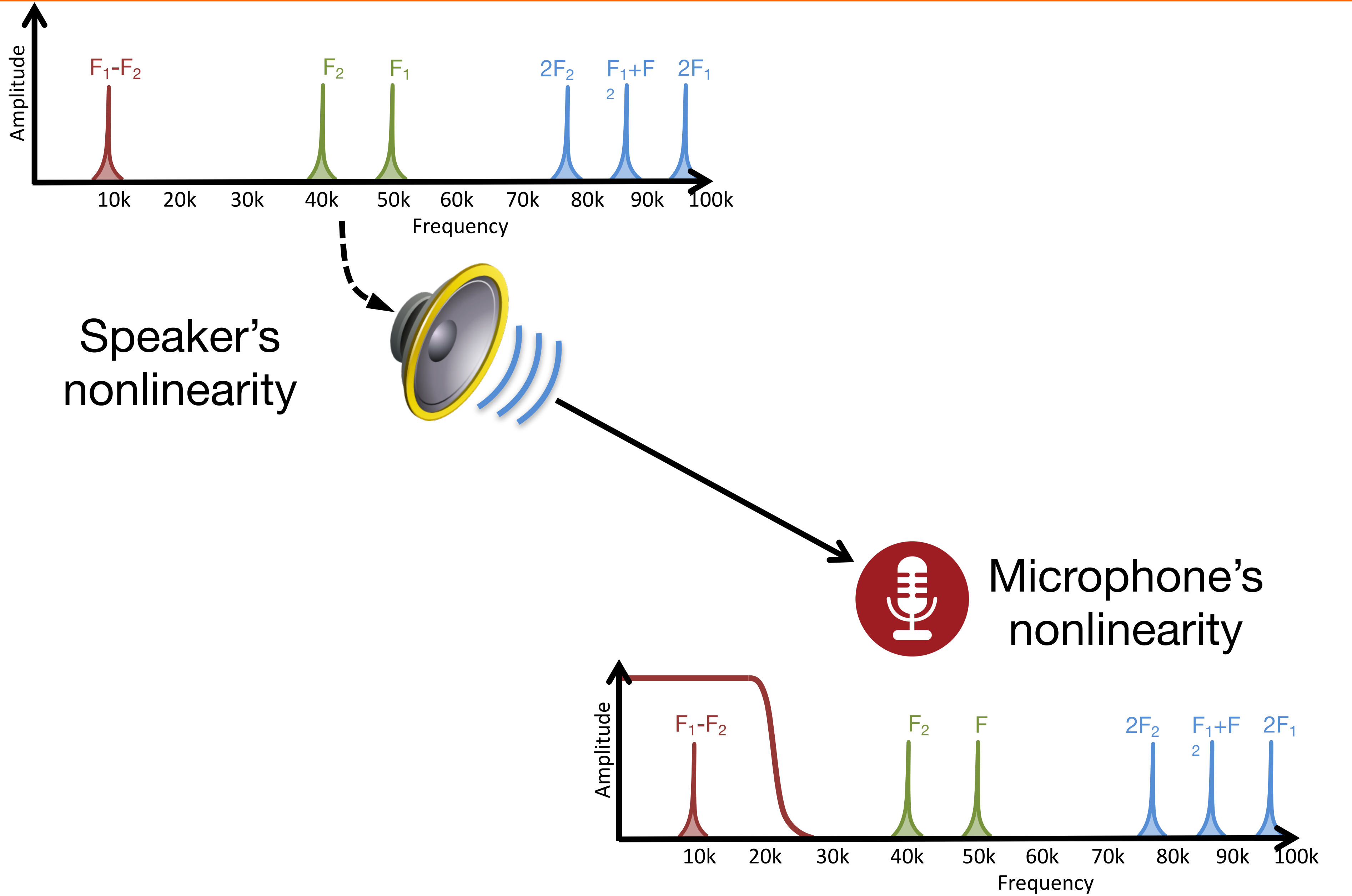
1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

Challenges



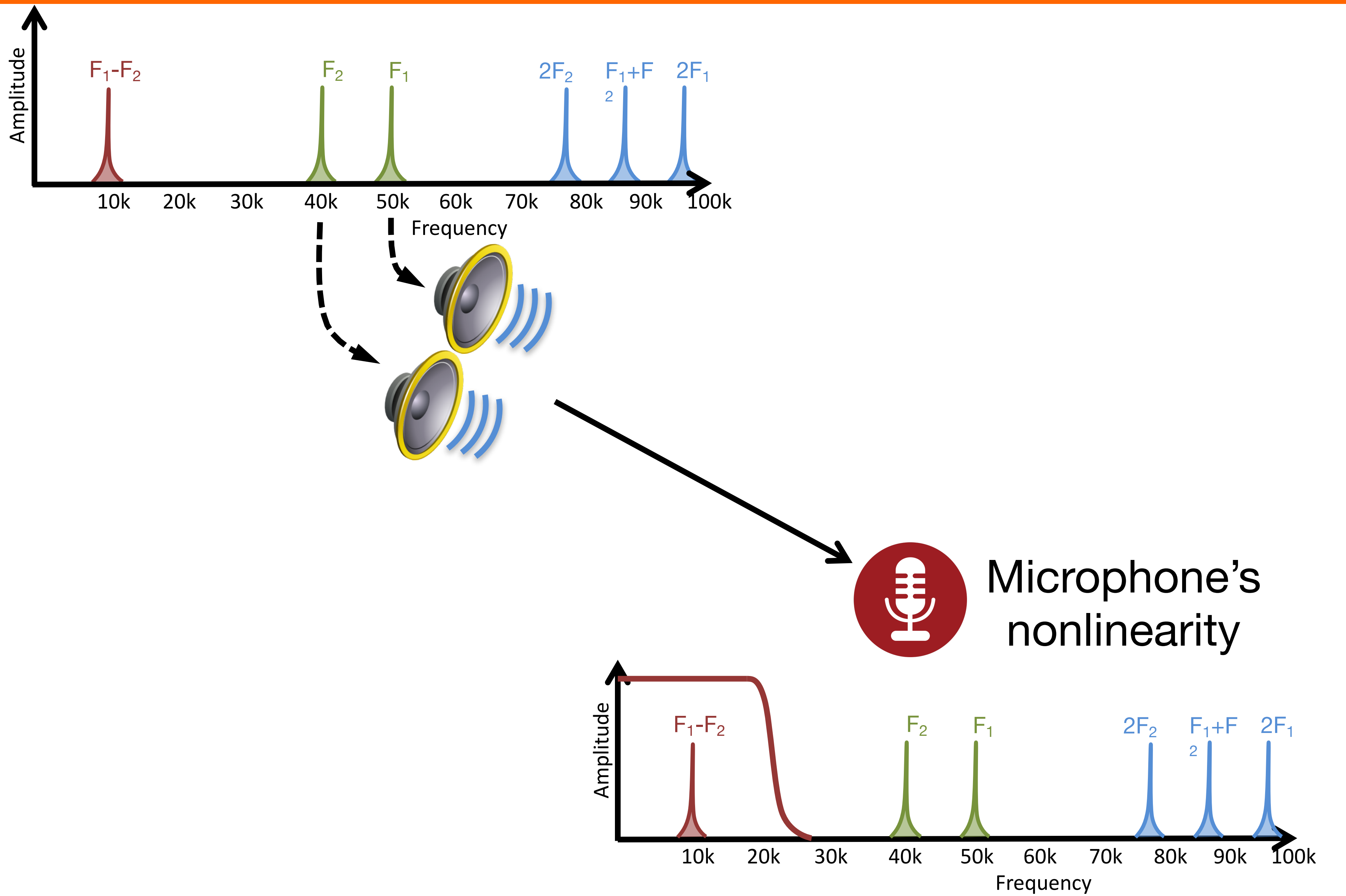
Amplitude
F2
F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency
Speaker's nonlinearity
Microphone's nonlinearity
Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency

Challenges

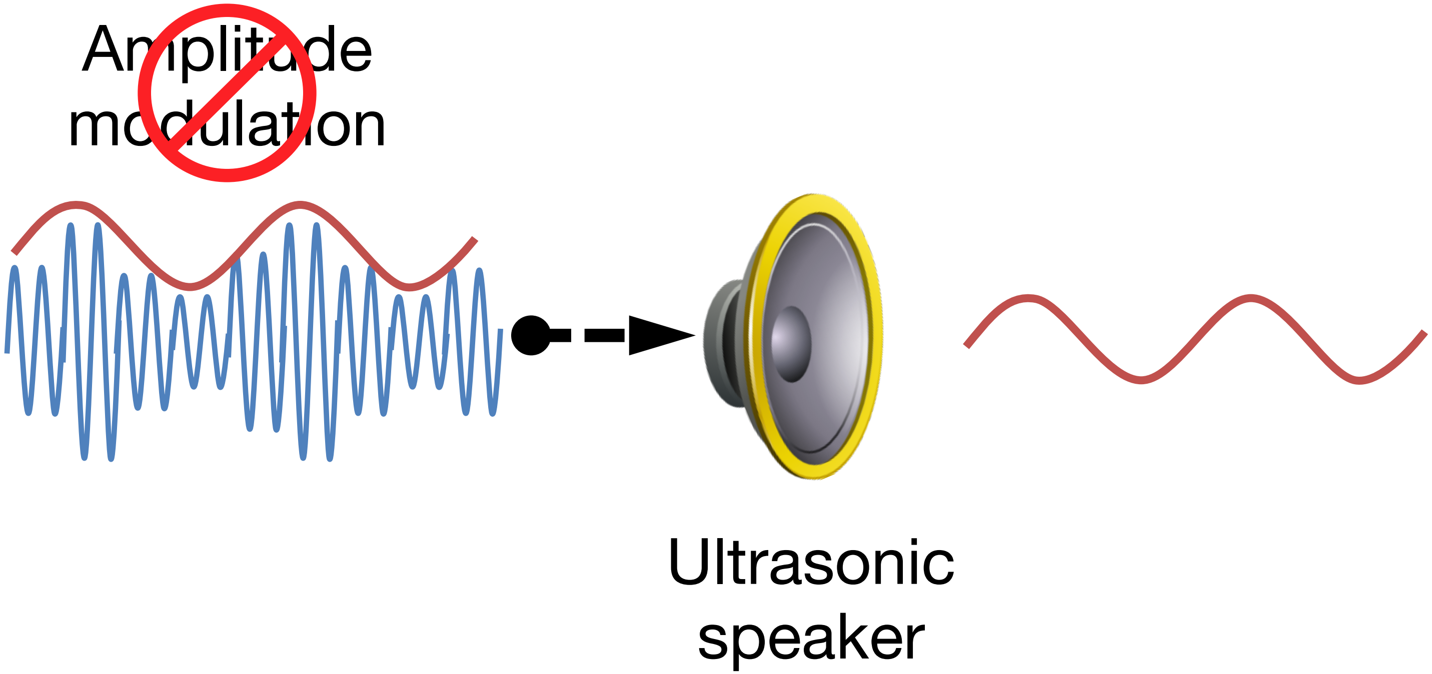


Amplitude
F_1-F_2
F_2
F_1
$2F_2$
F_1+F_2
$2F_1$
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency
Speaker's nonlinearity
Microphone's nonlinearity
Amplitude
F_1-F_2
F_2
F
$2F_2$
F_1+F_2
$2F_1$
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency

Challenges

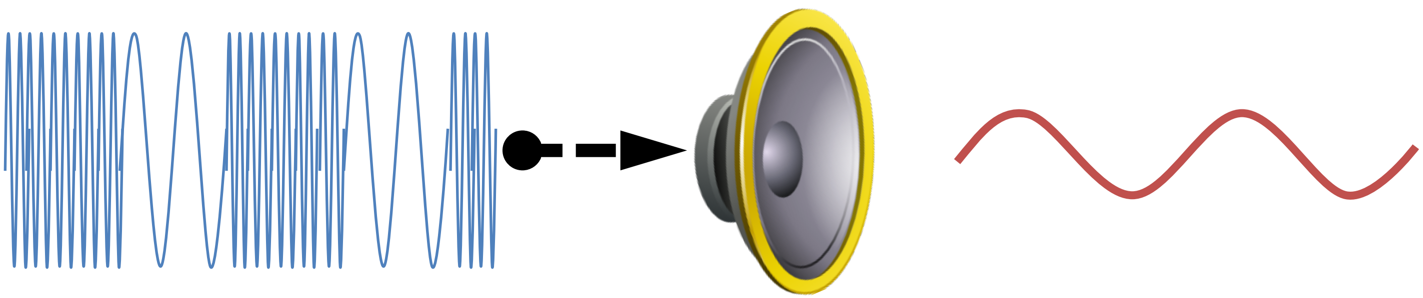

Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency
Microphone's nonlinearity
Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency

Challenges



Challenges

Frequency modulation



Ultrasonic speaker

Challenges

- Signal self-demodulation
- Piezoelectric ringing effect
- Carrier intermixing
- Spectrum inversion
- Carrier power allocation

Measurements and Validation

Sensitivity to High Frequencies:

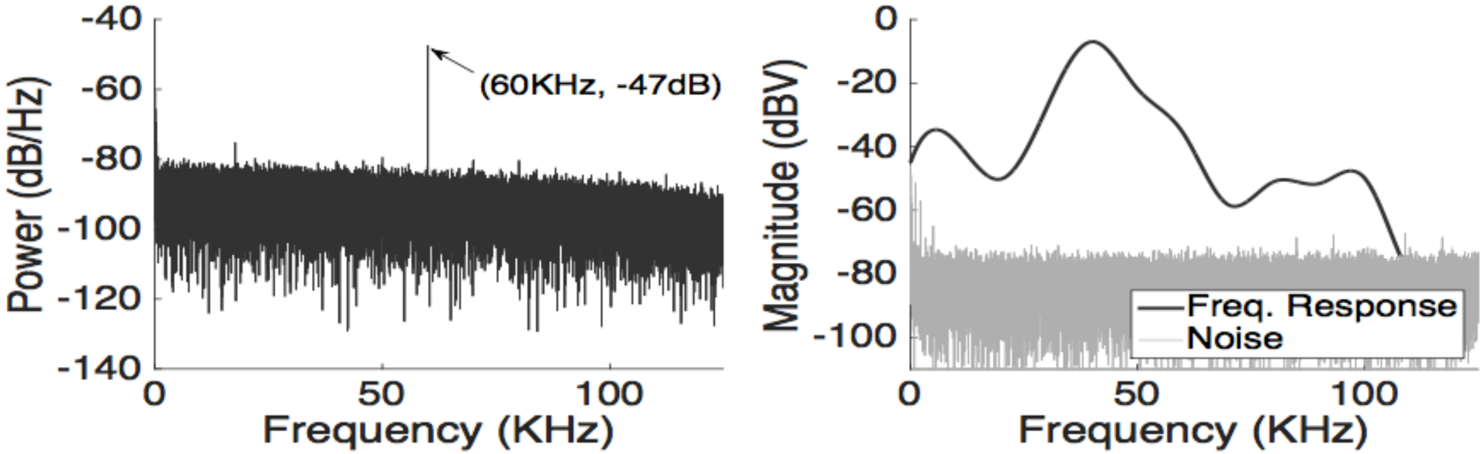


Figure 4: (a) Microphone signals (measured before the LPF) confirm the diaphragm and pre-amplifier's sensitivity to ultrasound frequencies. (b) Full freq. response at the output of the amplifier.

60kHz sound was played through an ultrasonic speaker and recorded with a programmable micro- phone circuit.

Measurements and Validation

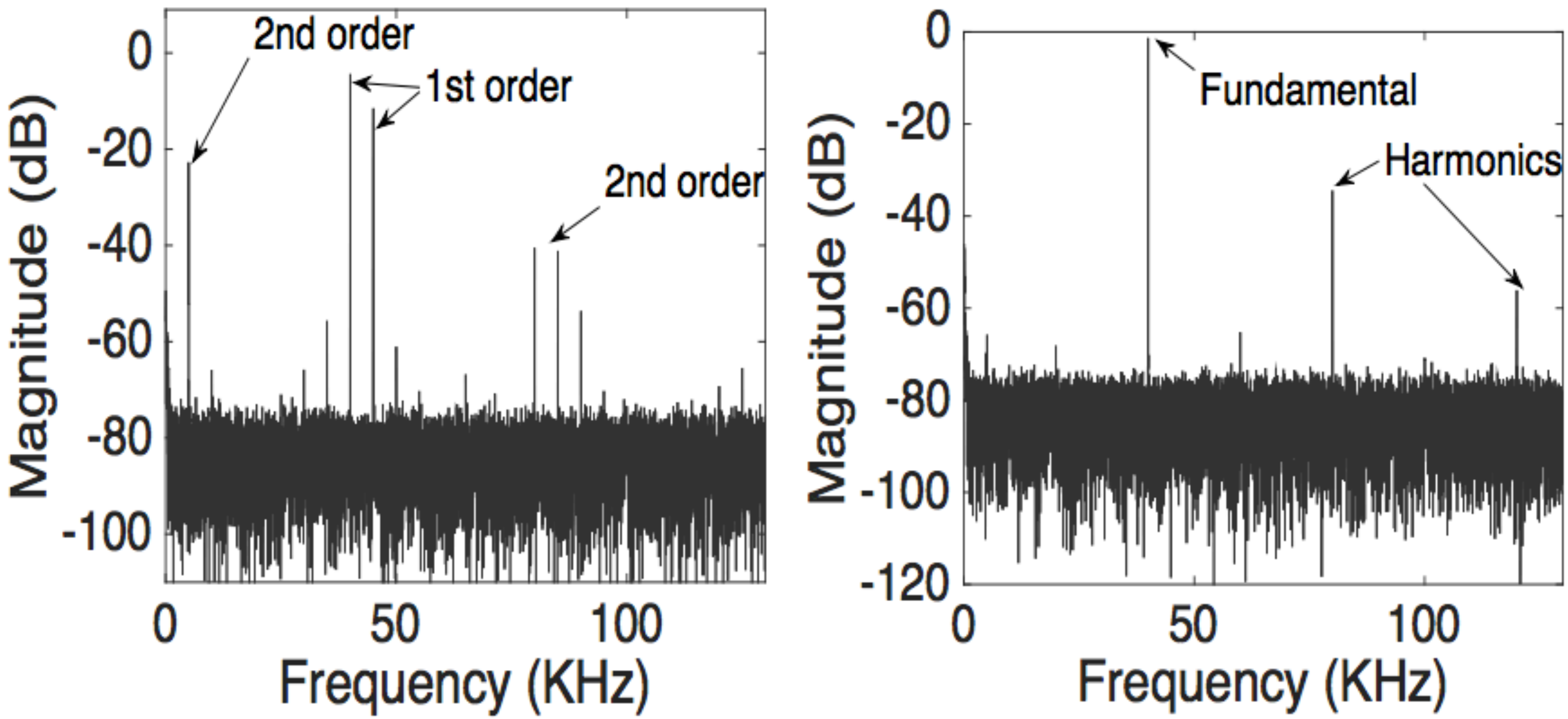
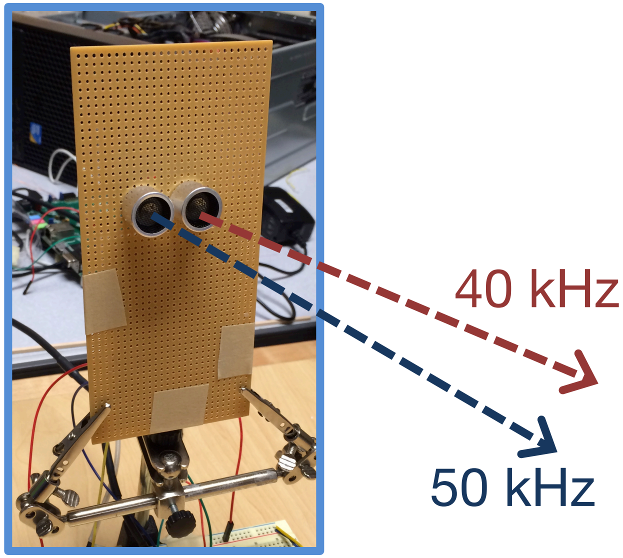
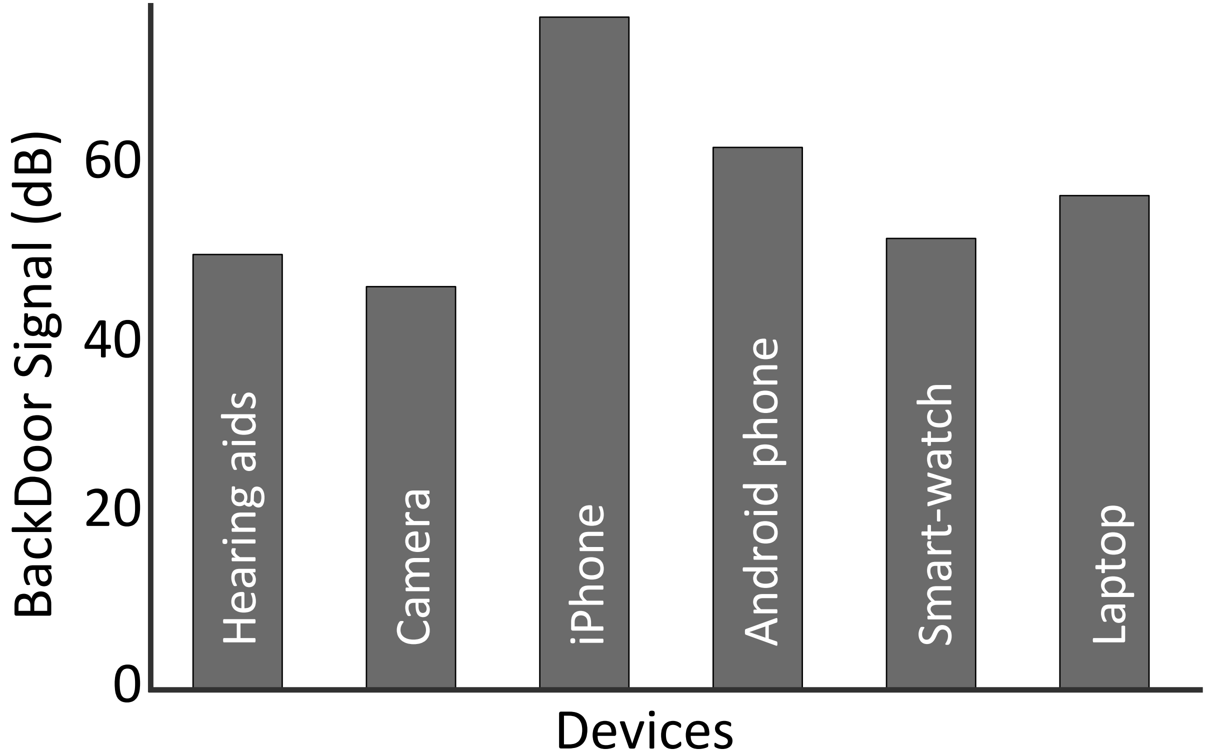


Figure 5: (a)The intermodulation distortion of signal (b) Harmonic distortion.

Hardware generalizability



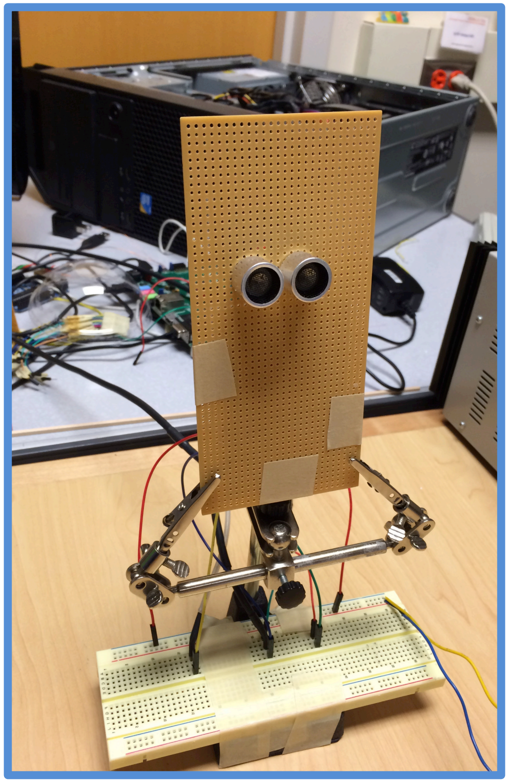


Hearing Aid | Camera | iPhone | Android phone | Smartwatch | Laptop

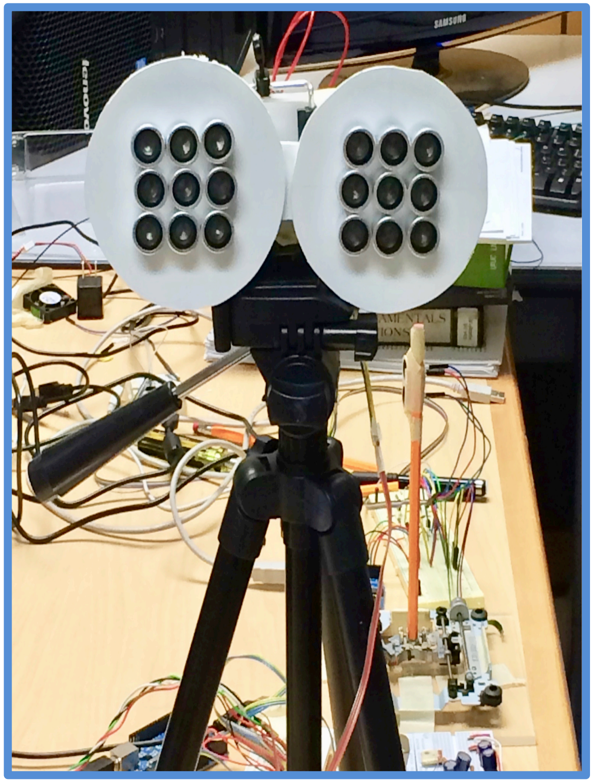
Talk outline

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

Implementation

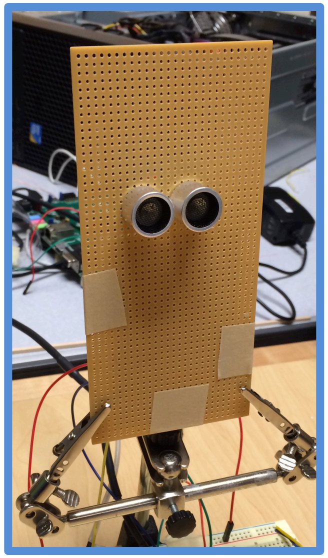


Communication prototype



Jammer prototype

Communication performance

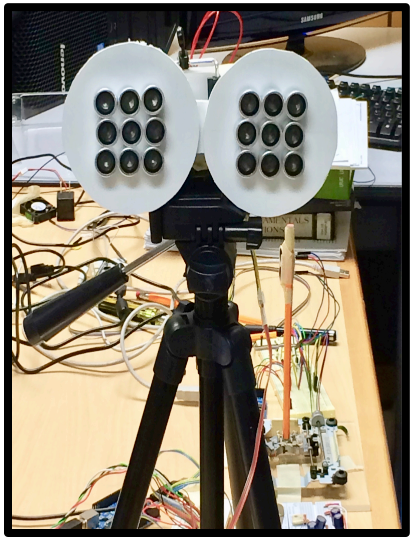


FM data packets

4kbps
up to 1 meter

More power can increase the distance

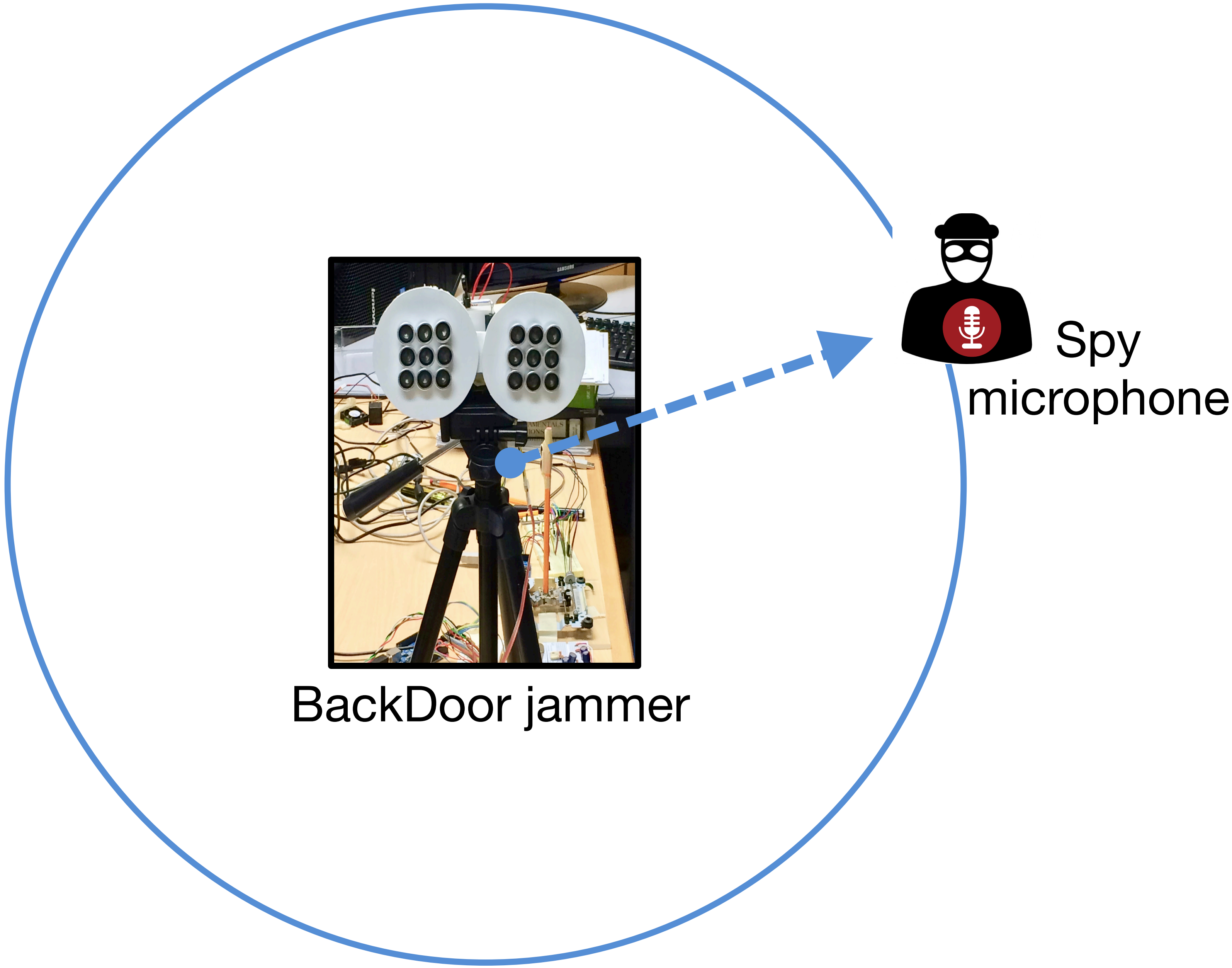
Jamming performance



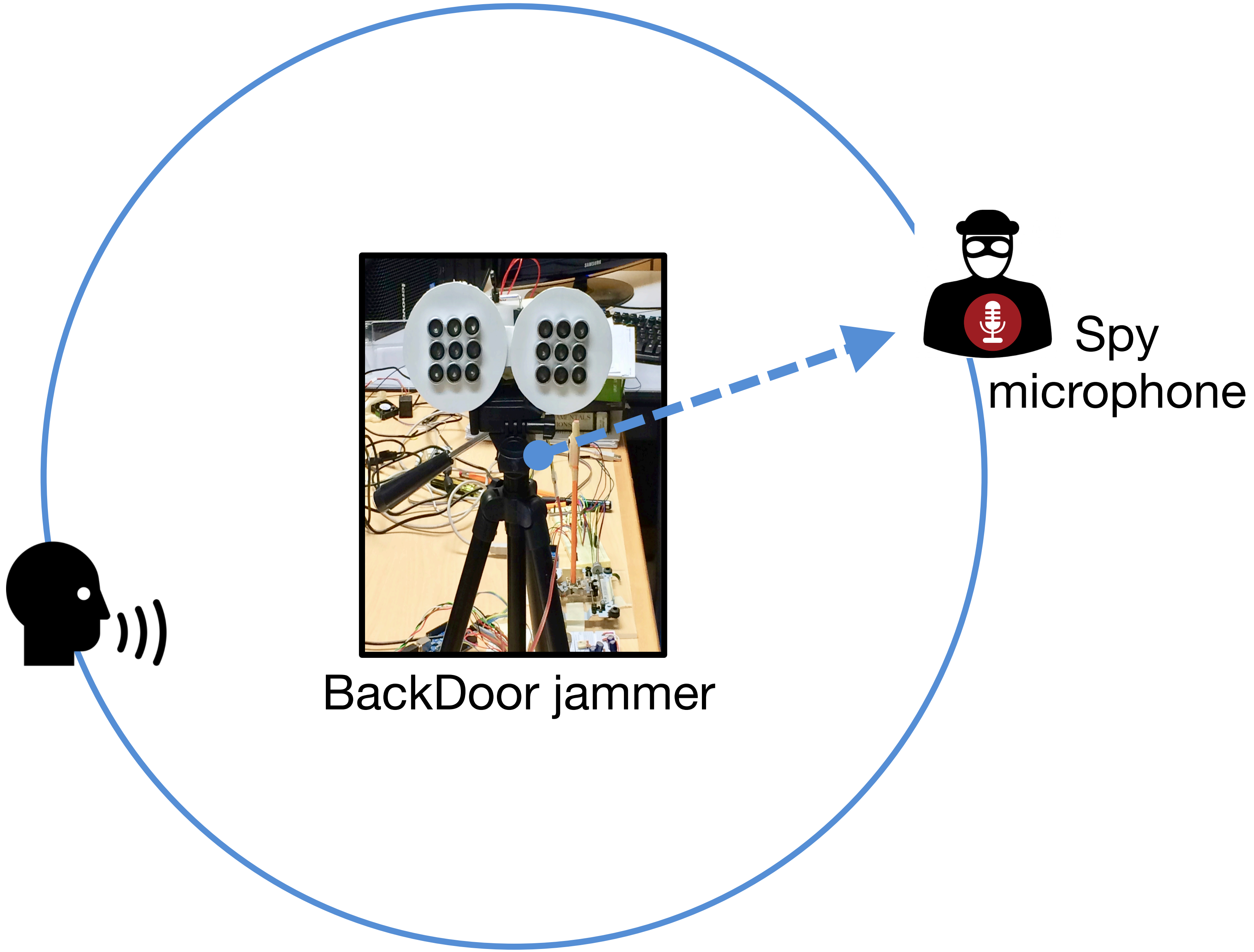
BackDoor jammer

Spy microphone

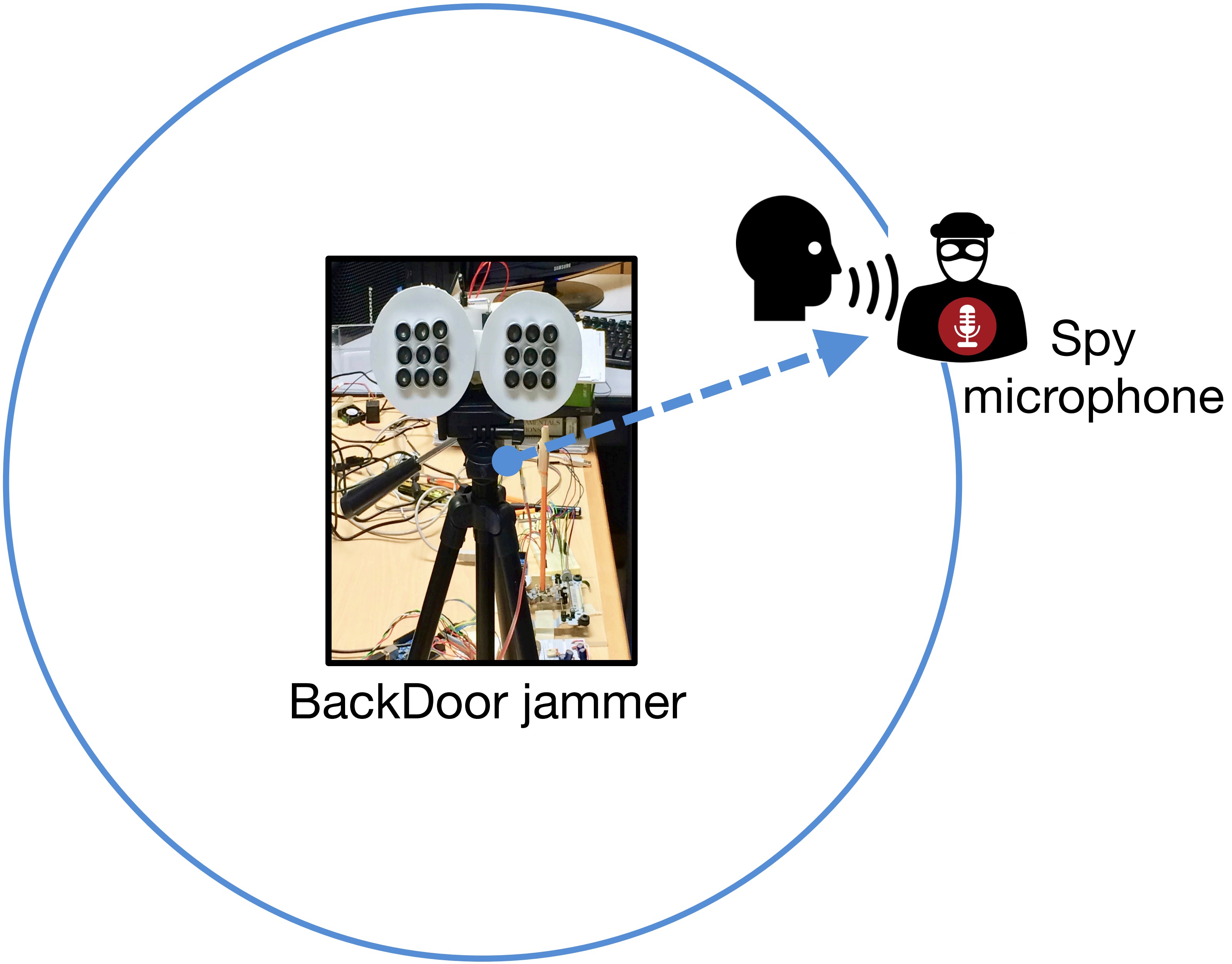
Jamming performance



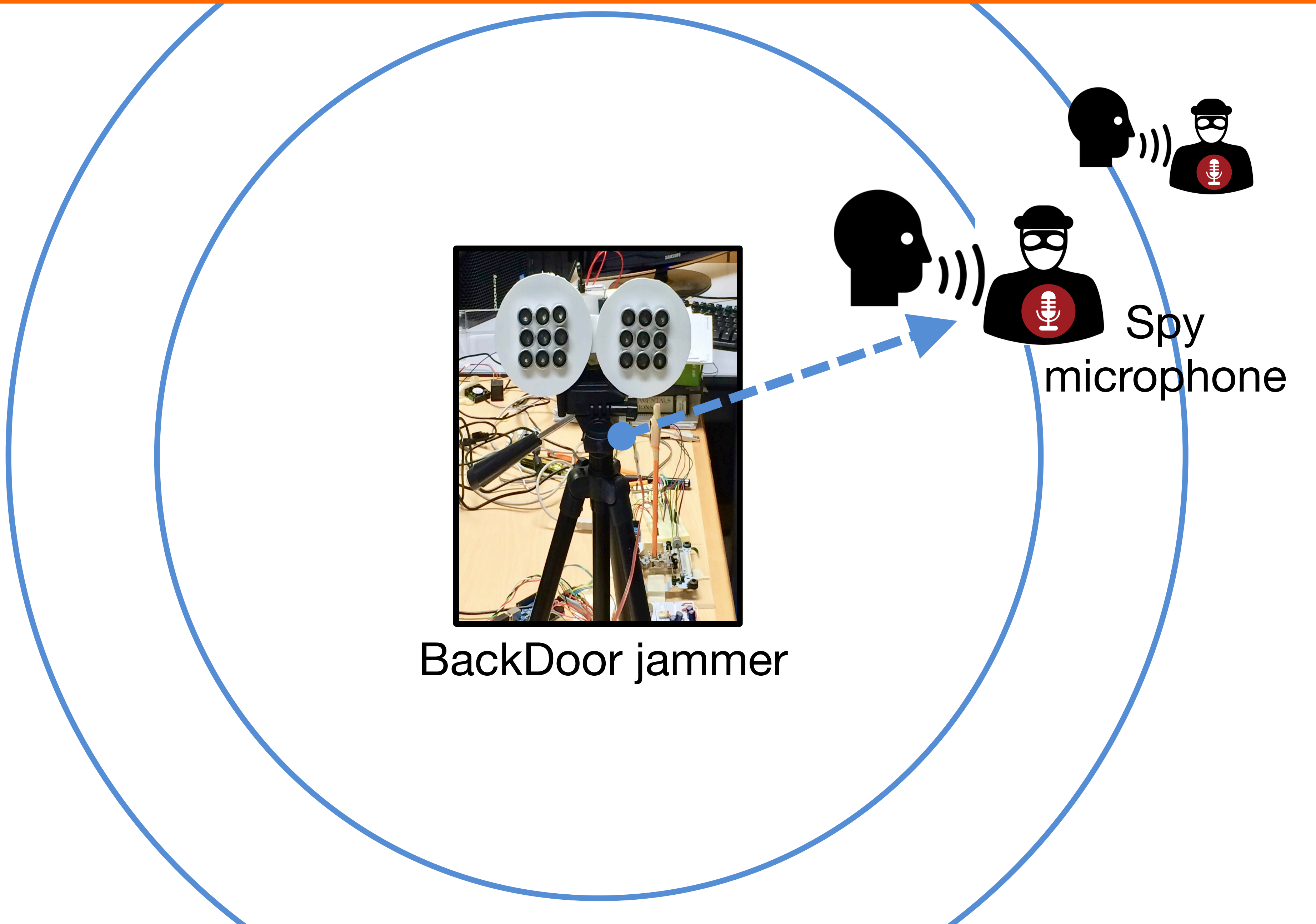
Jamming performance



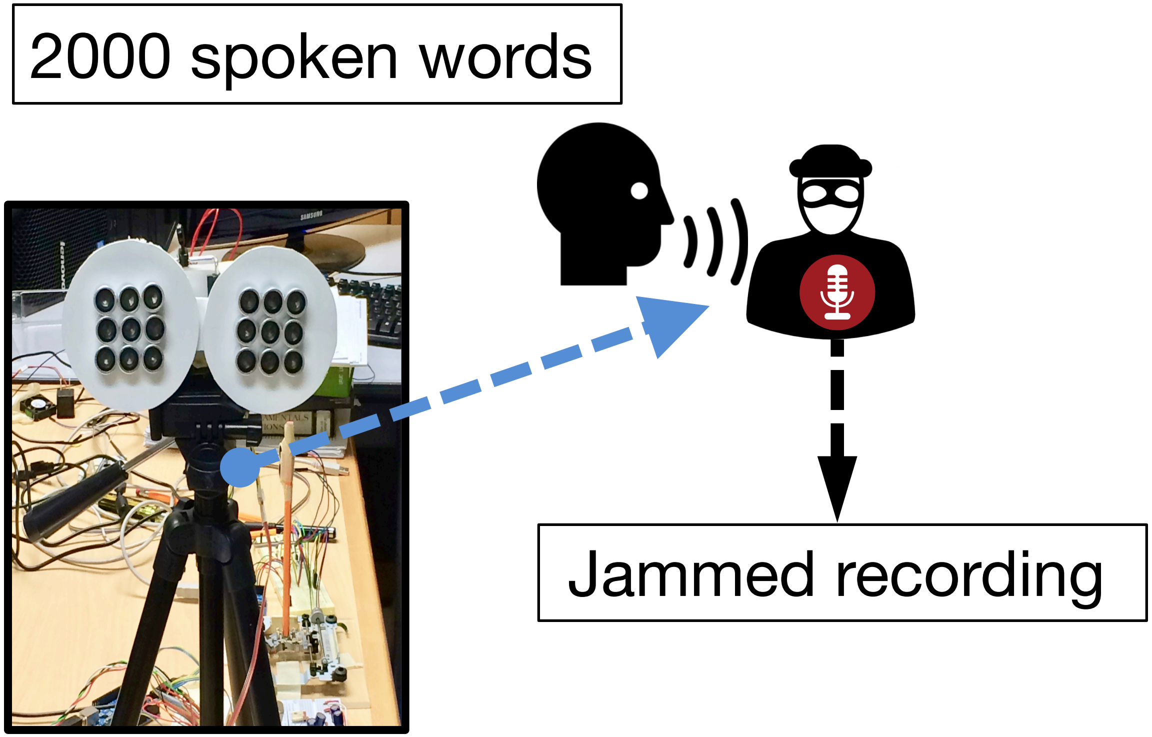
Jamming performance



Jamming performance

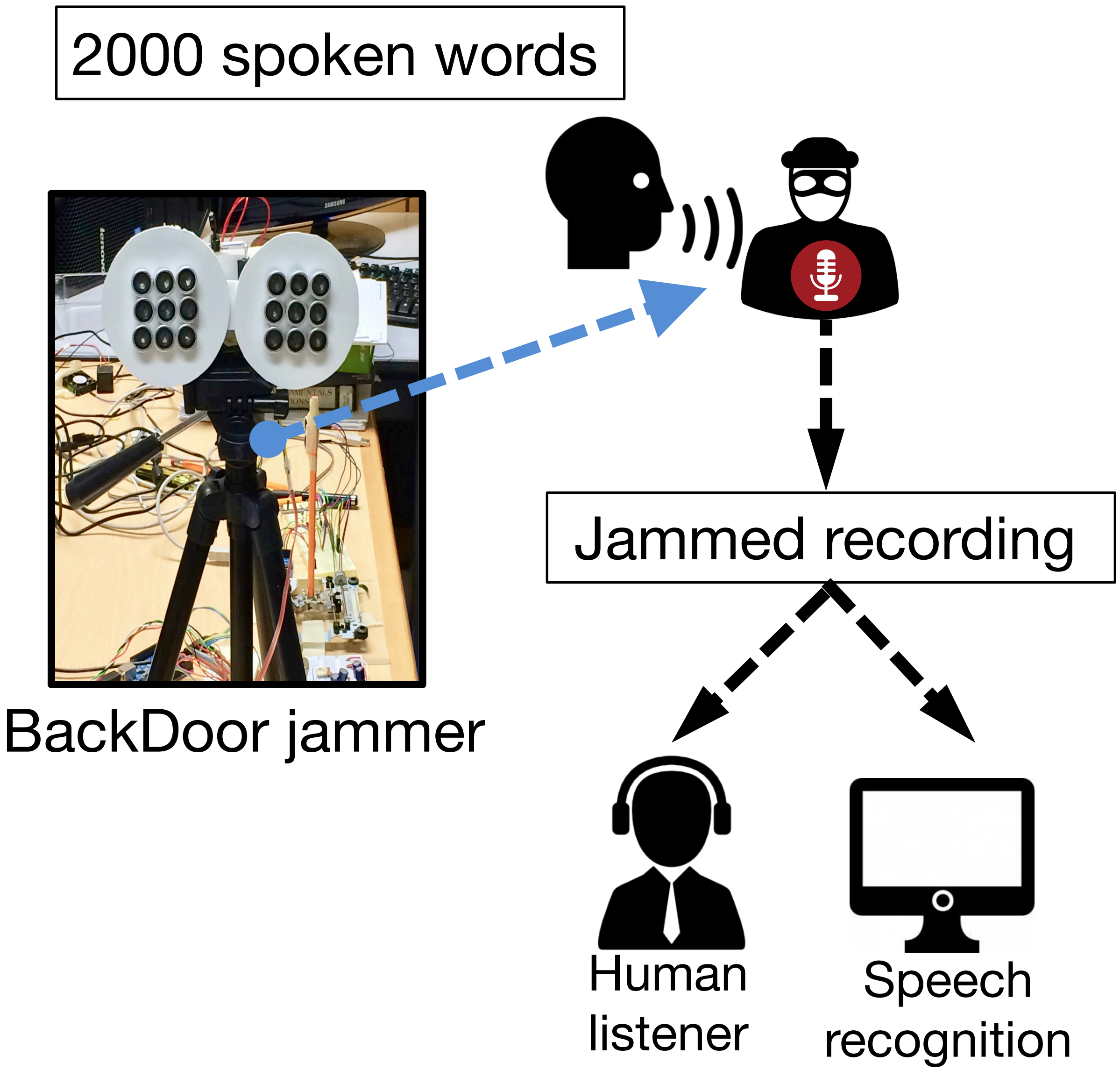


Jamming performance

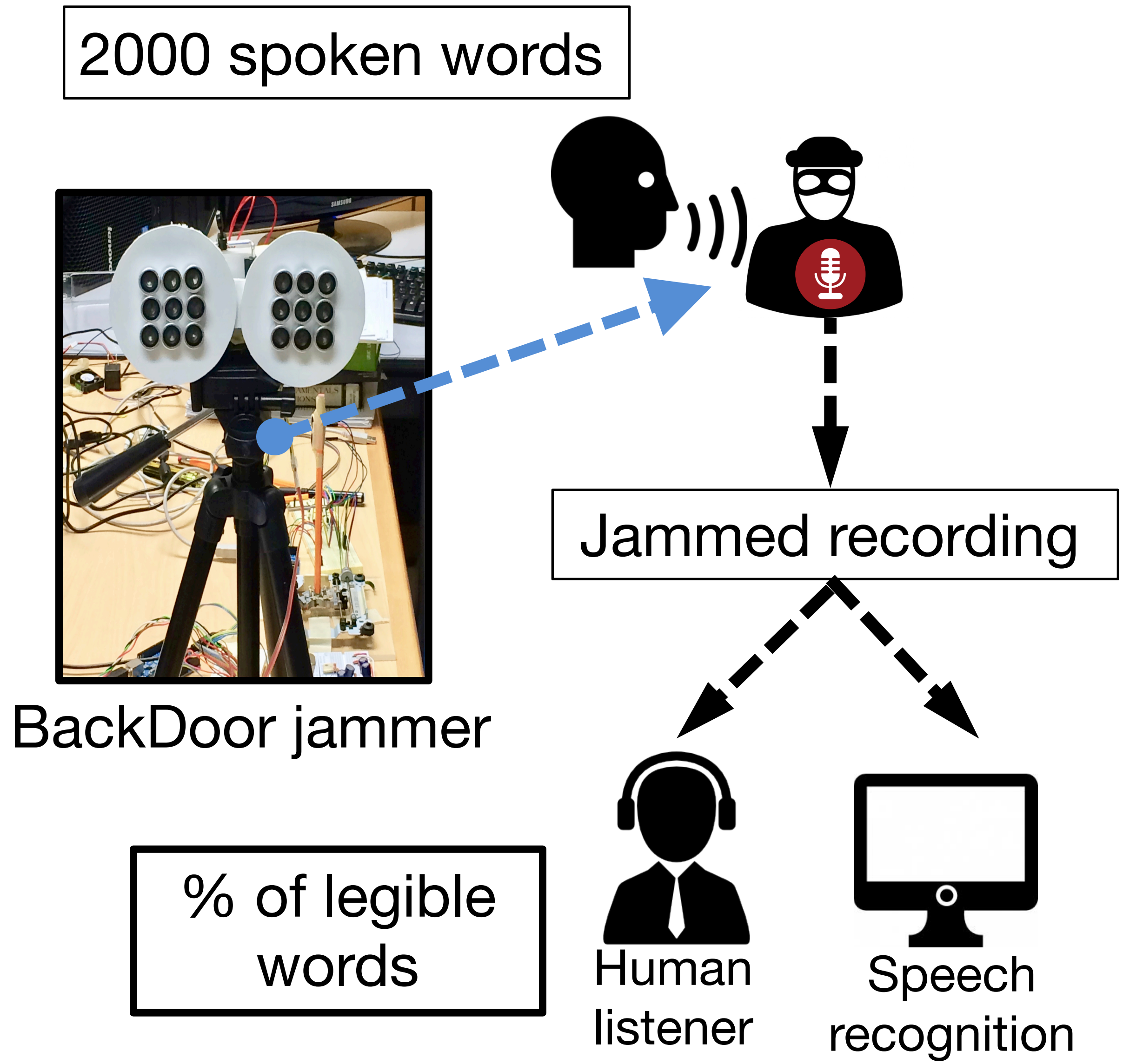


BackDoor jammer

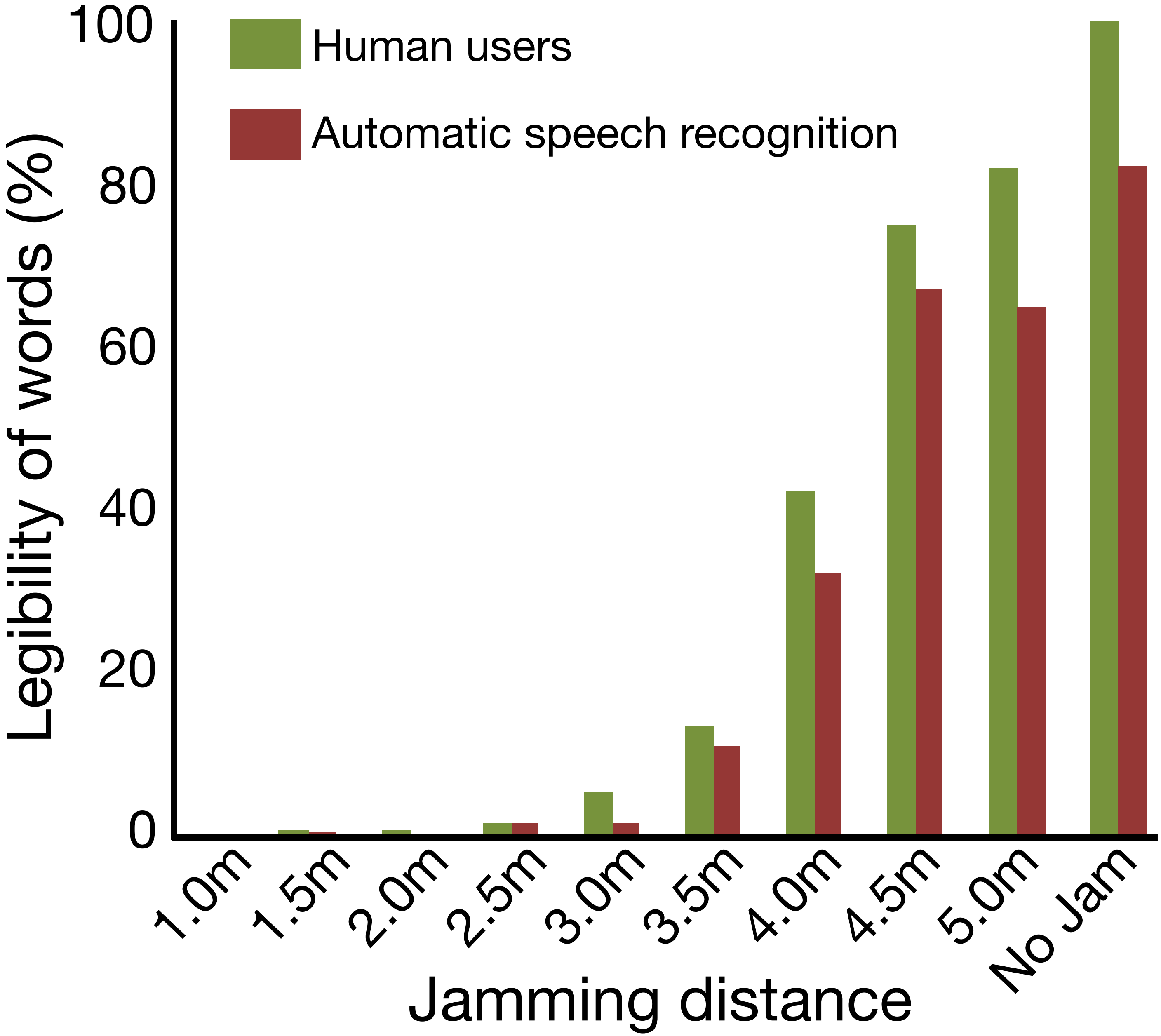
Jamming performance



Jamming performance



Jamming performance



Jamming performance

Takeaways

① Specially designed inaudible sound can be recorded with unmodified microphone

② It can make acoustic jammer possible and also can be a communication channel

③ It also uncovers threats like acoustic Denial-of-Service attacks

Thank You

SyNRG group website: http://synrg.csl.illinois.edu

Jamming performance