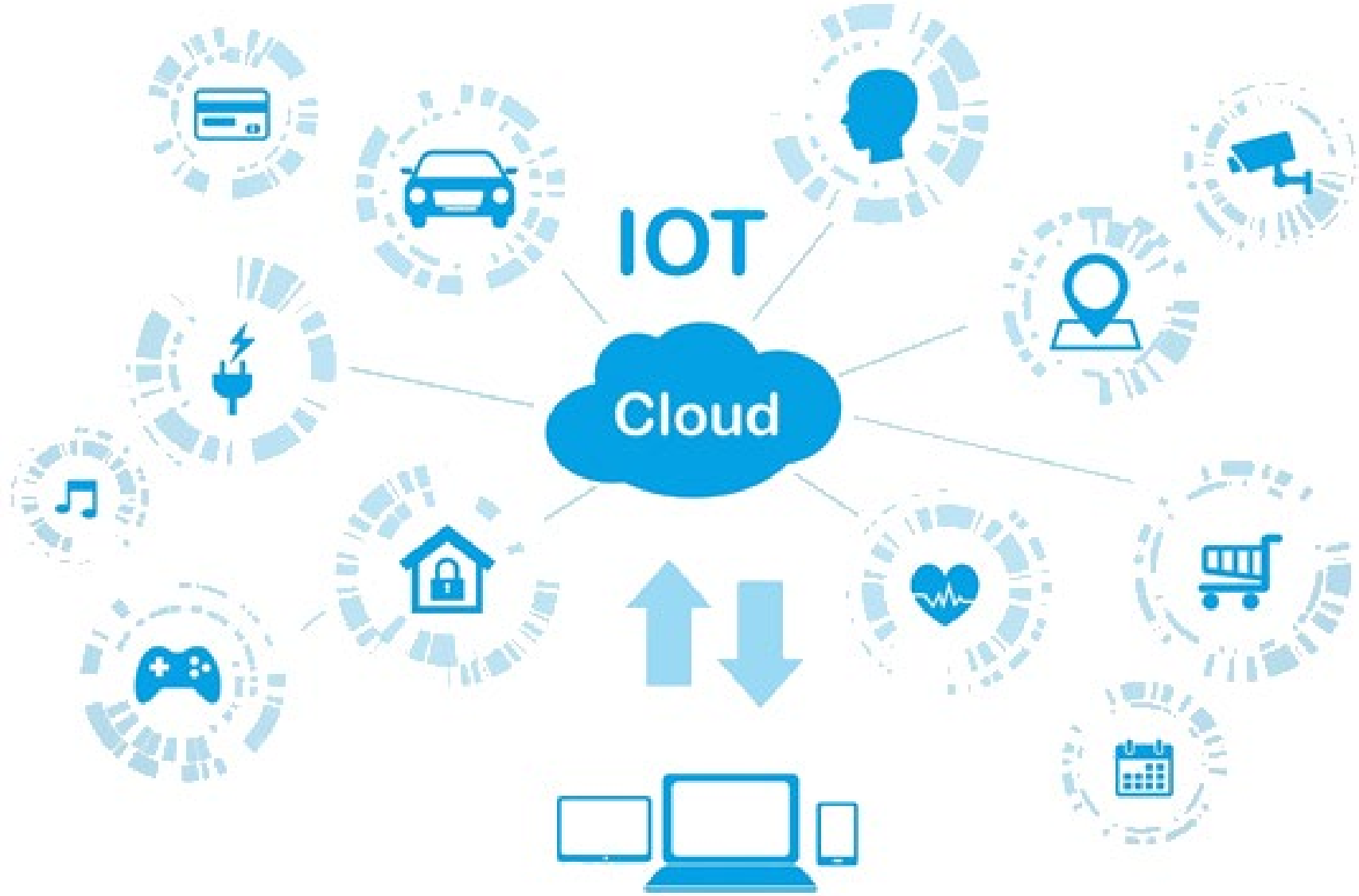
Deaf-Aid: Mobile IoT Communication Exploiting Stealthy Speaker-to-Gyroscope Channel

Ming Gao*, Feng Lin*, **Weiye Xu***, Muertikepu Nuermaimaiti*,
Jinsong Han*, Wenyao Xu^, Kui Ren

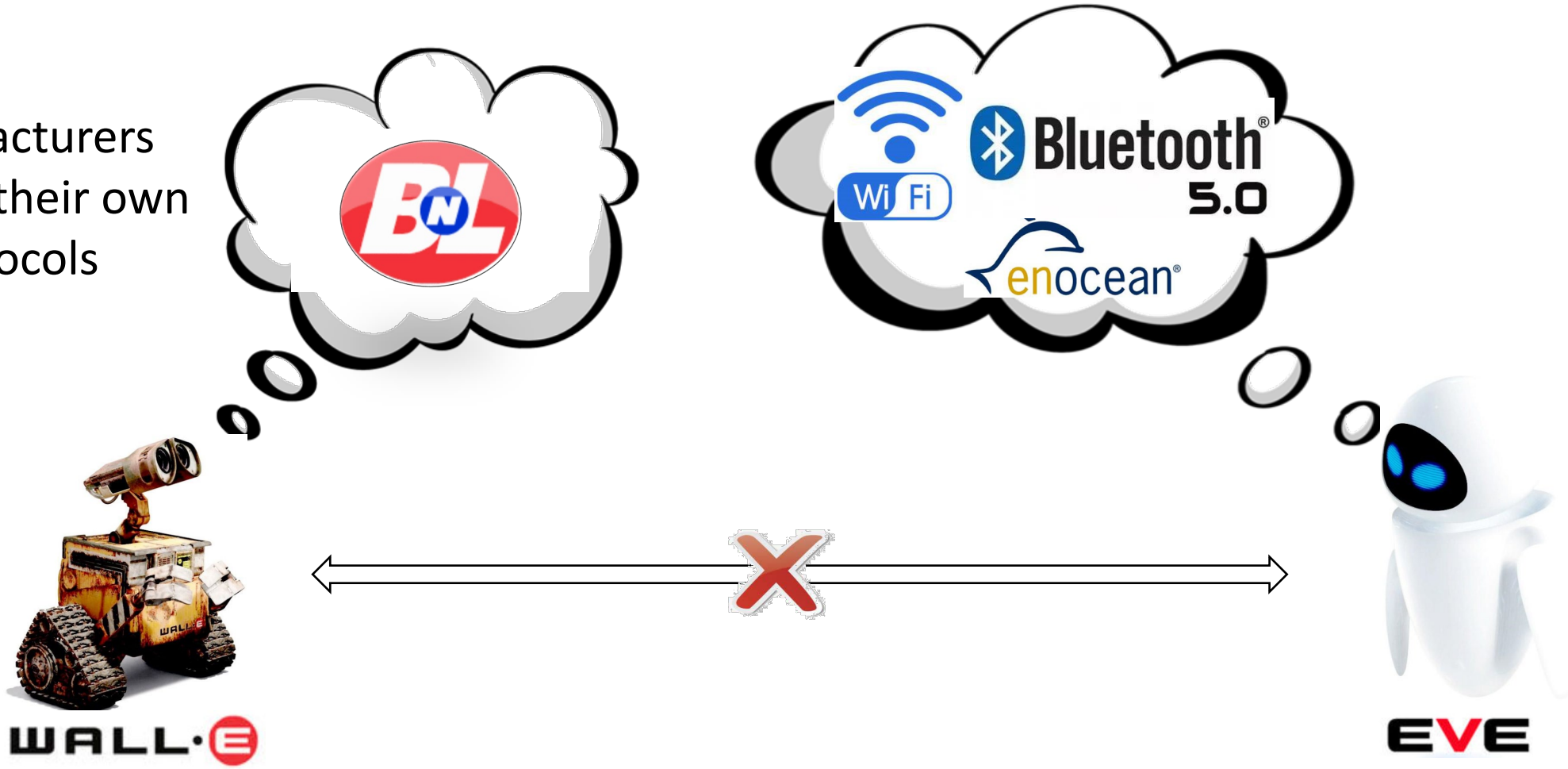
*Zhejiang University, Hangzhou, China

^SUNY Buffalo, New York, USA

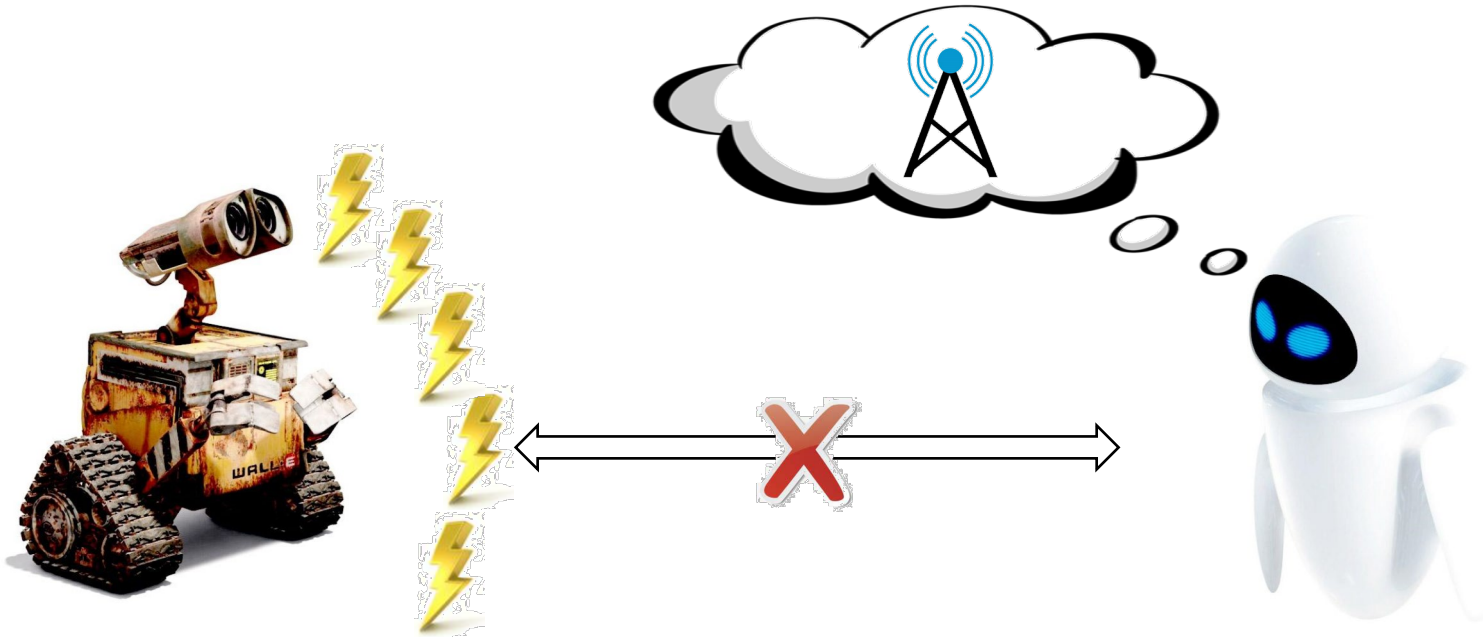


There are still many obstacles to realize such an everything-connected IoT network!

Manufacturers develop their own protocols

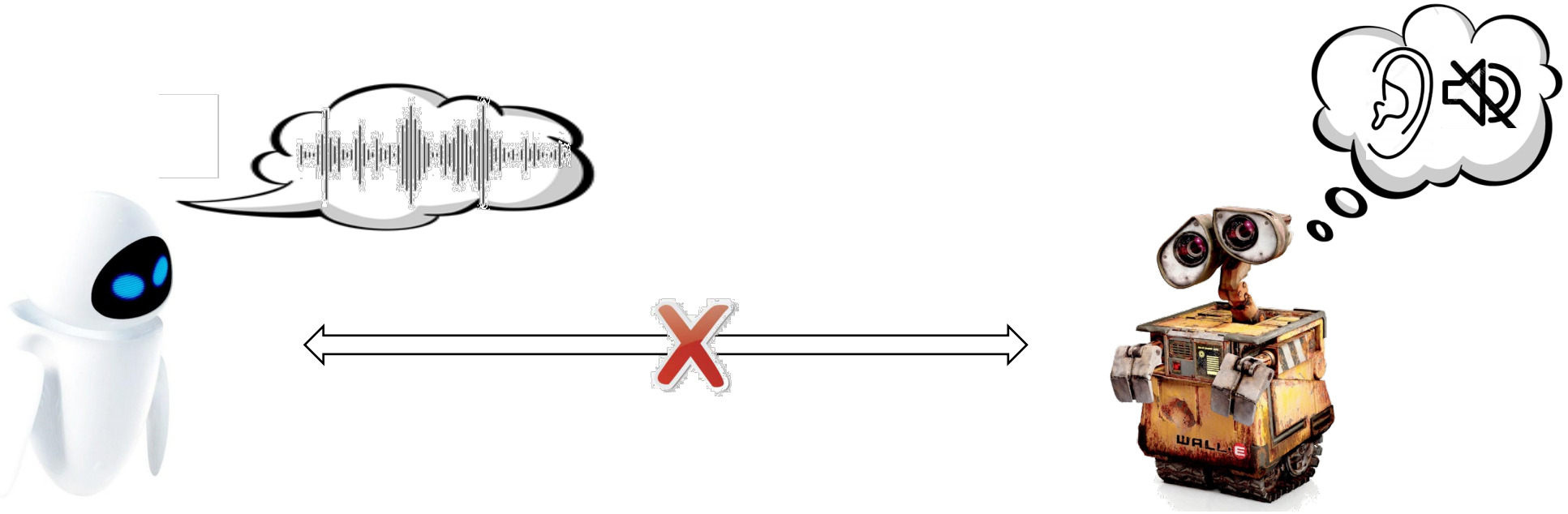


Incompatible protocols make it impossible for WALL.E to communicate with EVE!



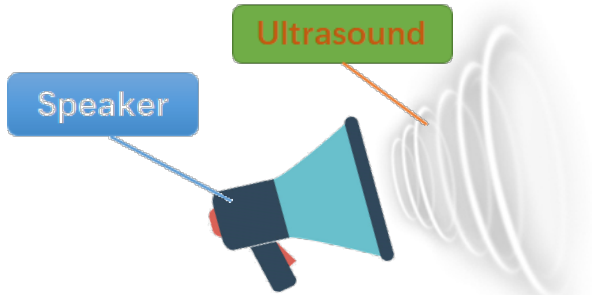
Communication means based only on the electromagnetic wave would fail upon the electromagnetic interference and shielding!

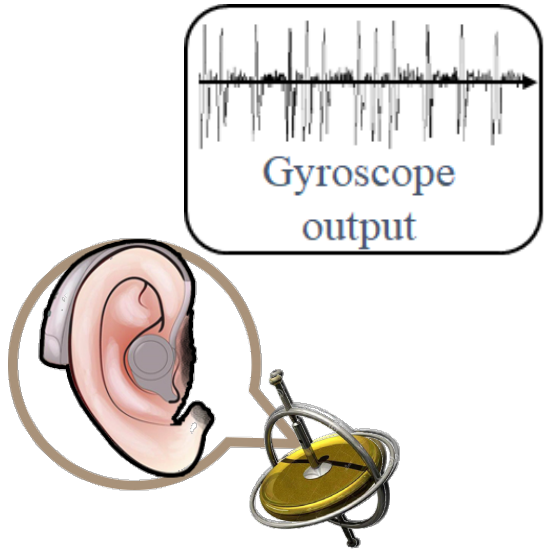
Paired transmitter-receiver are always required.



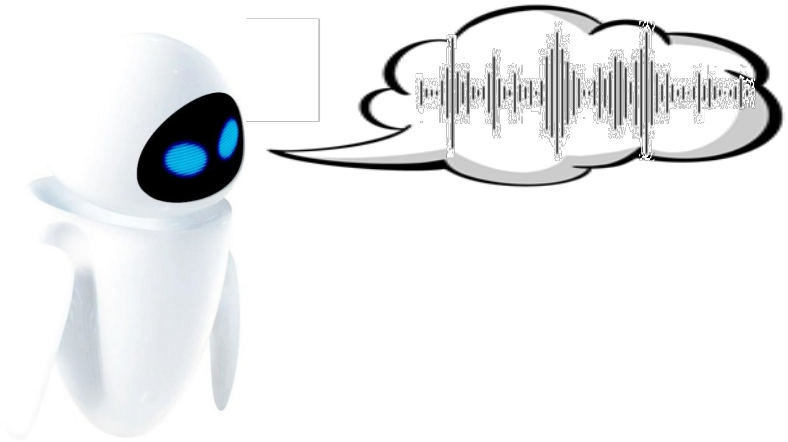
Our vision

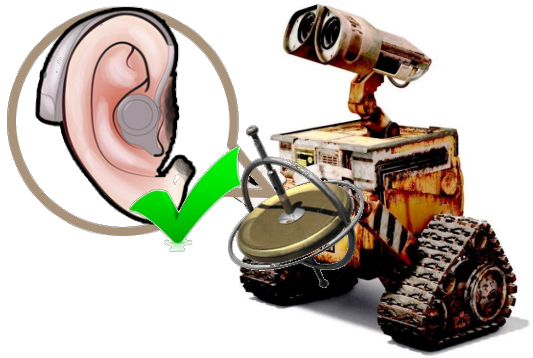
- Protocol-independent
- No Peripheral
- Robust to Movement



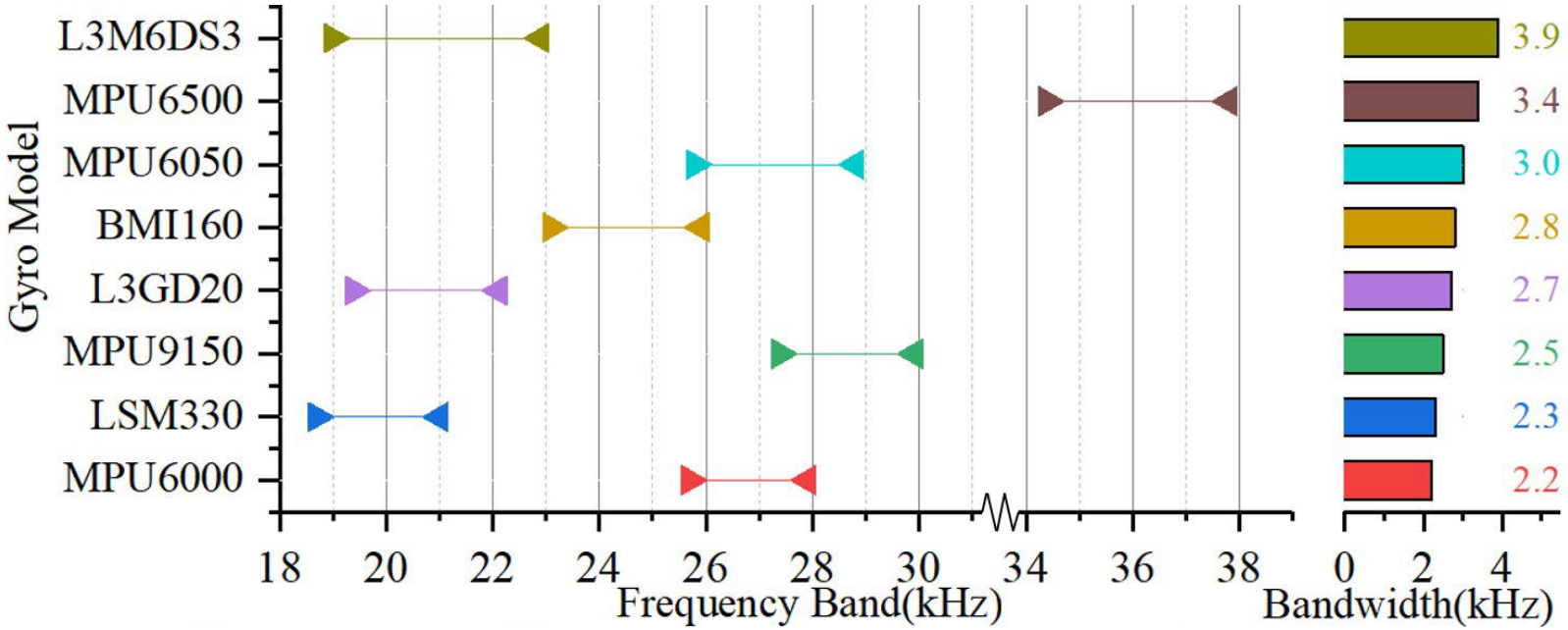


It provides a complementary communication channel to current IoT devices.



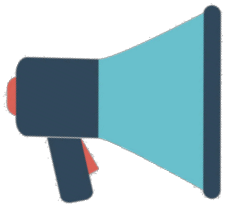


Feasibility Study



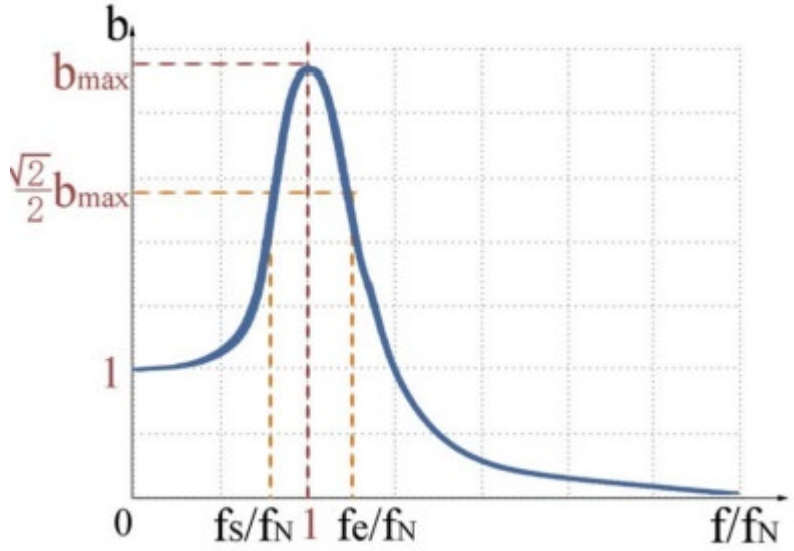
- ✓ Non-contact
- ✓ Inaudibility
- ✓ No peripheral

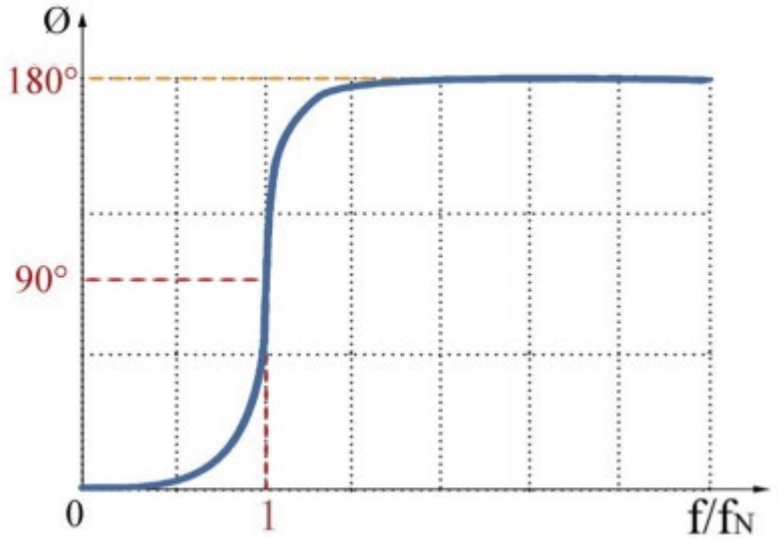
$$F(t) = A \cdot sin(2\pi f_0 t + \phi_0)$$



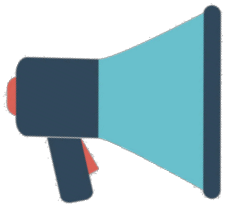
$$M = F(t) - F(t + t_{pw}) + F(t + \triangle t) - F(t + \triangle t + t_{pw})$$

$$R_0(t) = bA \cdot sin(2\pi f_0 t + \phi_0 + \phi_1)$$



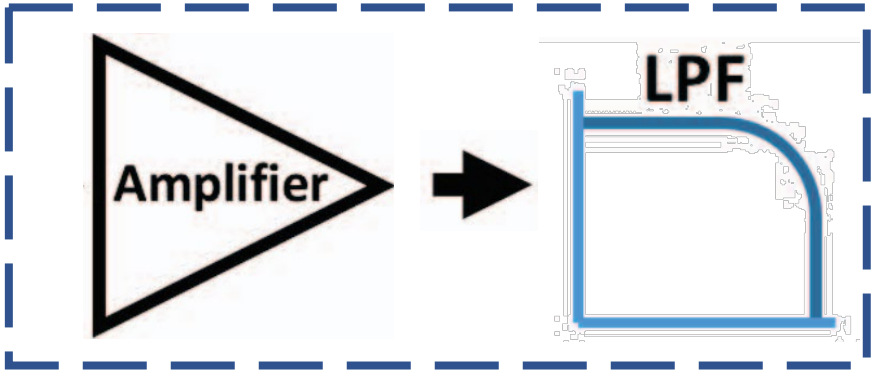


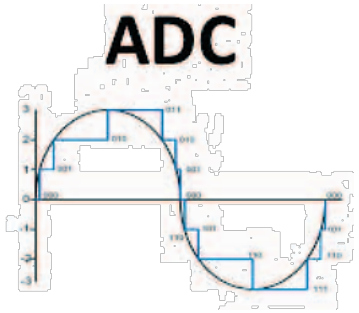
$$F(t) = A \cdot sin(2\pi f_0 t + \phi_0)$$



$$M = F(t) - F(t + t_{pw}) + F(t + \triangle t) - F(t + \triangle t + t_{pw})$$

$$R_0(t) = bA \cdot sin(2\pi f_0 t + \phi_0 + \phi_1)$$





$$R(t) = bLA \cdot sin(2\pi f_0' t + \Phi)$$

$$\Phi = \phi_0 + \phi_1 + \phi'$$

$$f_0' = n \times Fs + f_1 \quad (-\frac{Fs}{2} < f_1 < \frac{Fs}{2})$$

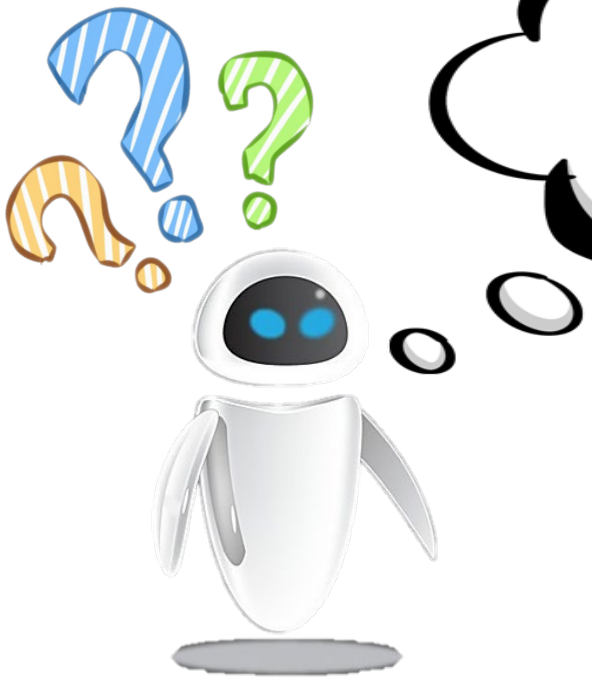
$$R[k] = bLA \cdot sin(2\pi f_1 \frac{k}{Fs} + \Phi)$$

System Overview

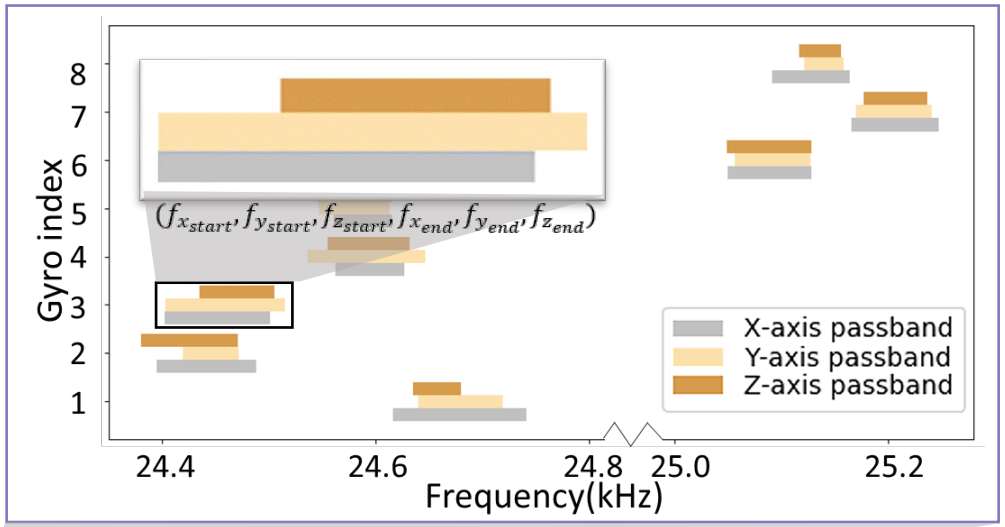
1. How to identify the receiver?

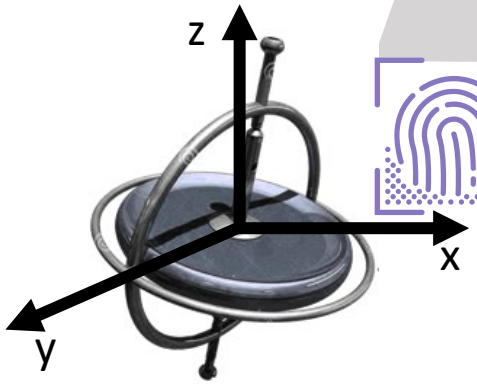
2. How to ensure high-quality communication?

3. How to suppress motion influence?



How to distinguish WALL.E from his brothers?

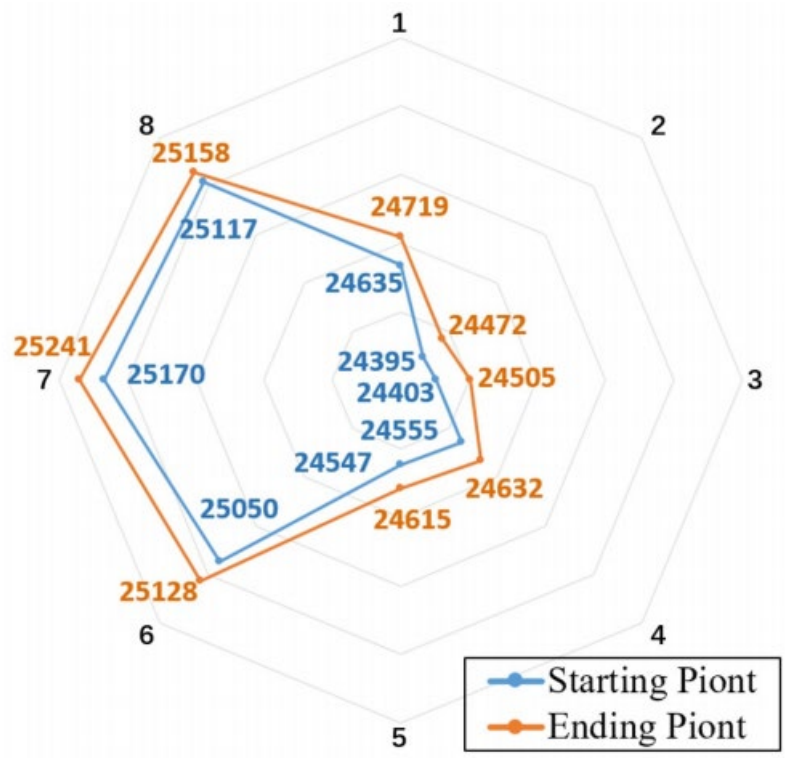




ID range

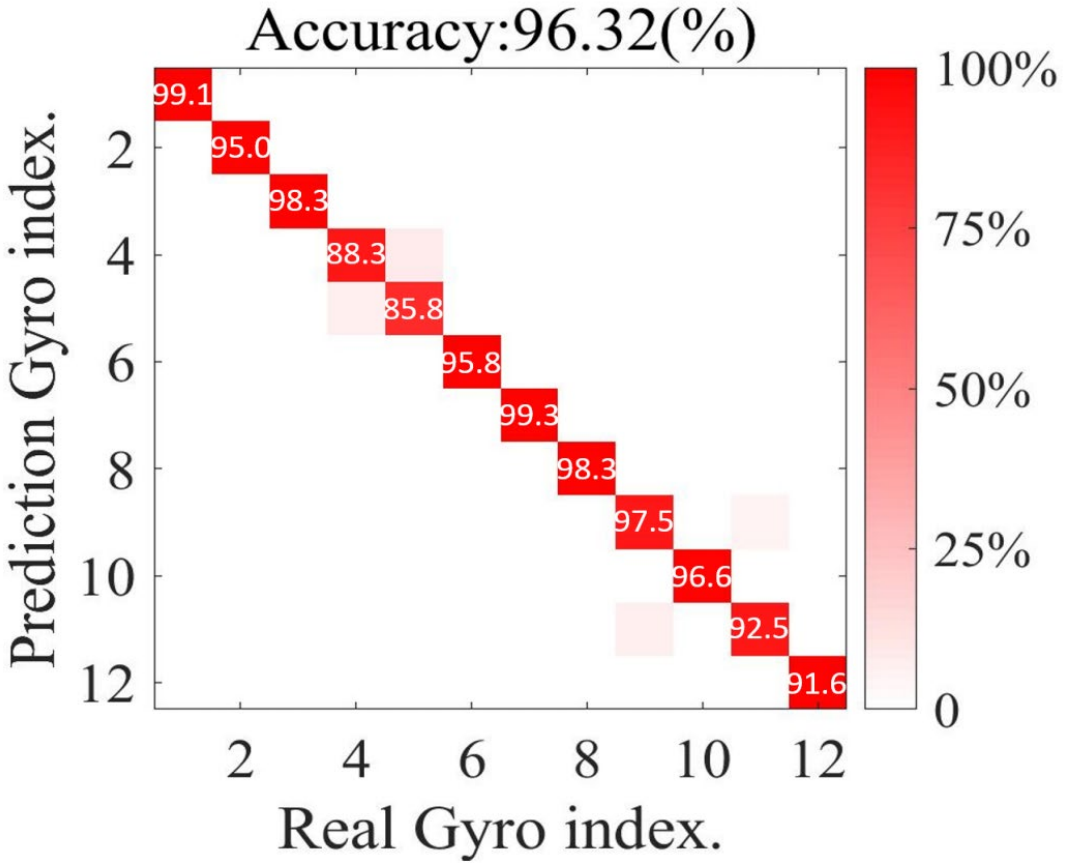
Deaf-Aid leverages the diversity of resonant passband of gyroscope as device fingerprint to identify receivers

ID Range



$$[\text{Median}(f_{x_{start}}, f_{y_{start}}, f_{z_{start}}), \text{Median}(f_{x_{end}}, f_{y_{end}}, f_{z_{end}})]$$

- We tested 6 speakers and 12 gyroscopes
- It achieves an accuracy of 96.32% totally.

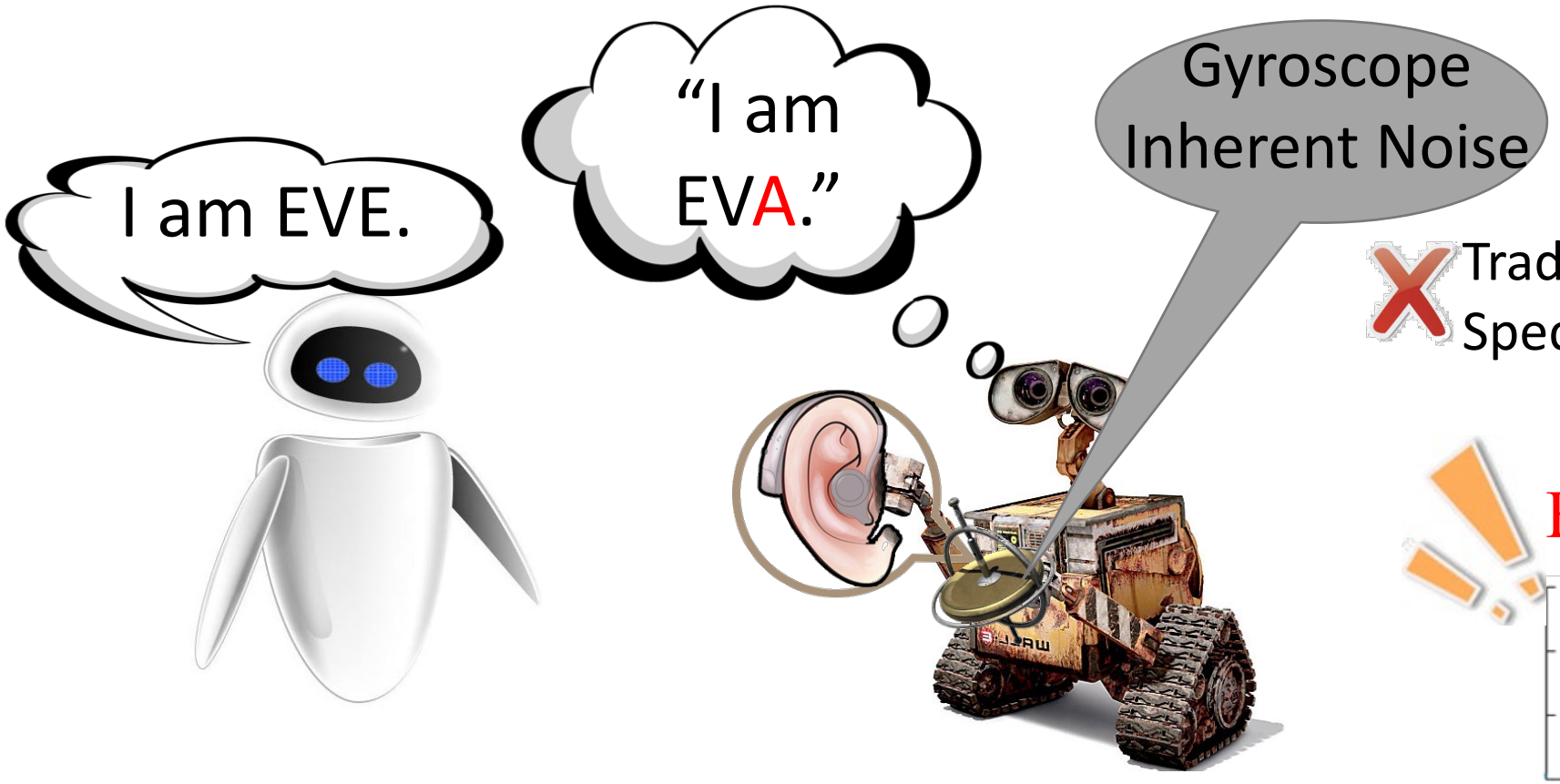


System Overview

1. How to identify the receiver?

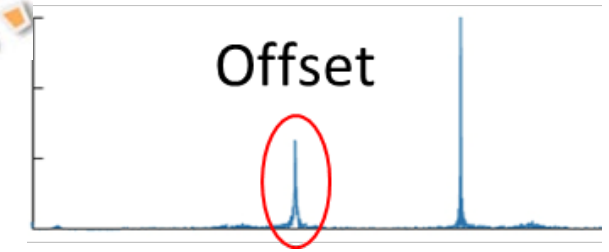
2. How to ensure high-quality communication?

3. How to suppress motion influence?



✗ Traditional anti-noise techniques: Spectrum analysis

Frequency offset



$$f_0' = n \times (Fs + \Delta Fs) + f_2$$

$$R[k] = bLA \cdot sin(2\pi f_2 \frac{k}{Fs + \Delta Fs} + \Phi)$$

Solution: Multiplier-based Correction

Our Observation:

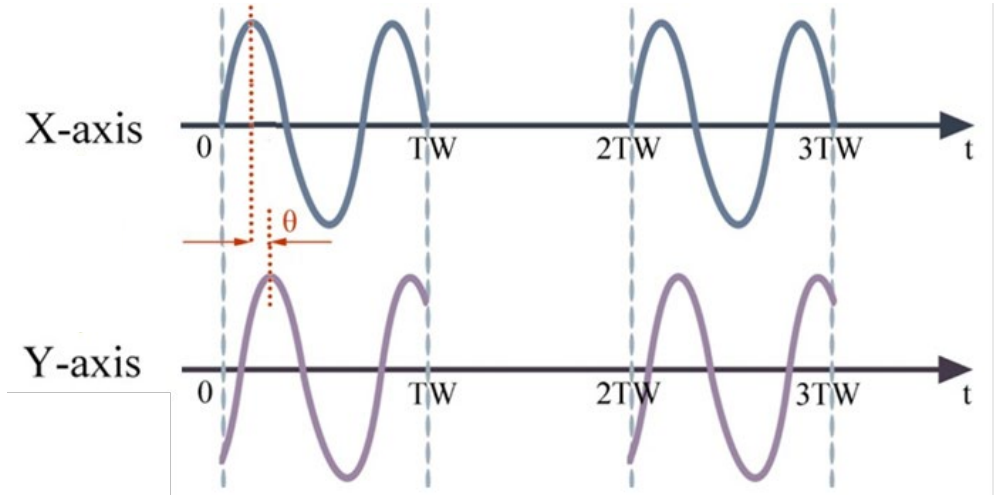
- Frequency synchronization
- Fixed phase difference

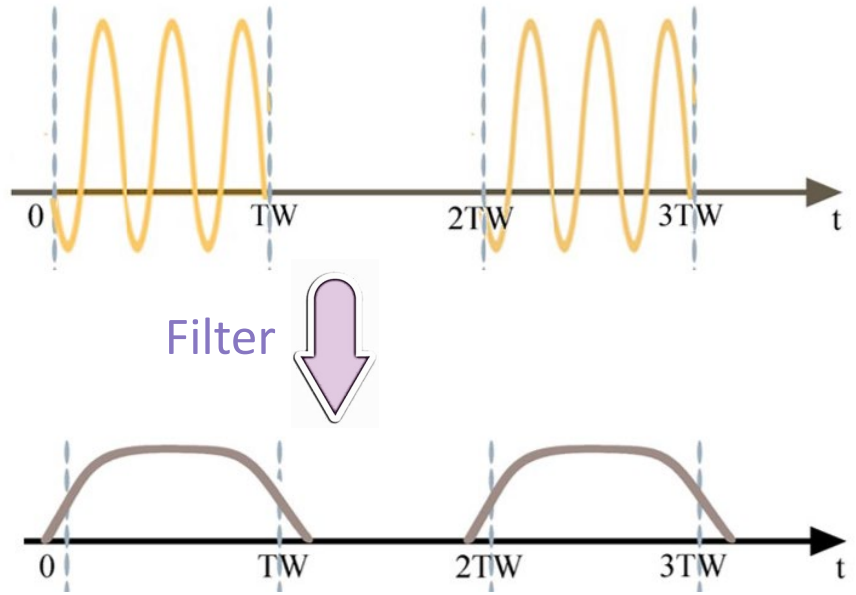
$$S_{cor}[k] = R_x[k] \times R_y[k]$$

$$= \frac{1}{2} A_x A_y \boxed{cos(\Phi_x - \Phi_y)}$$

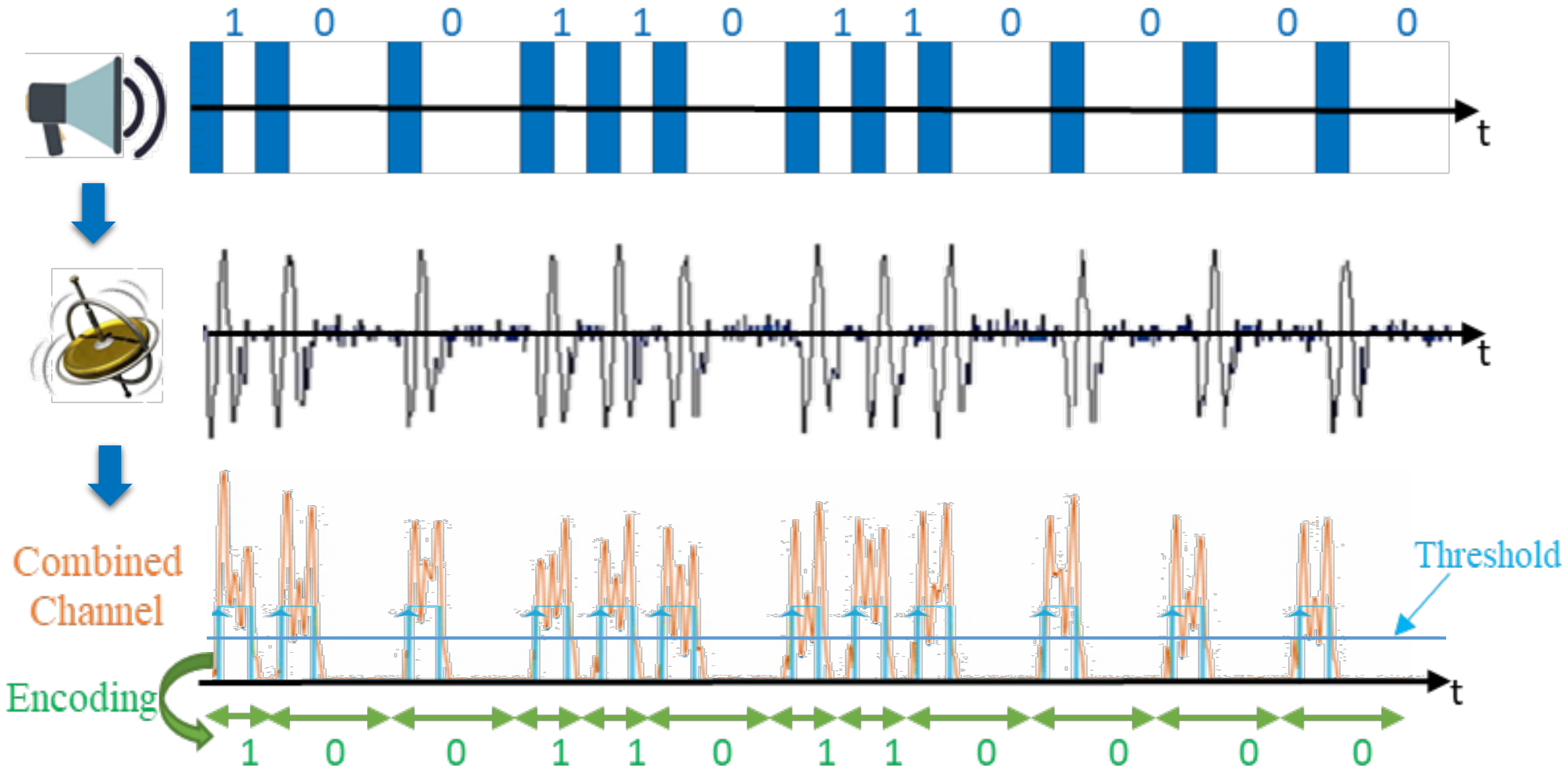
Constant!

Noise is removed in an offset-independent way.



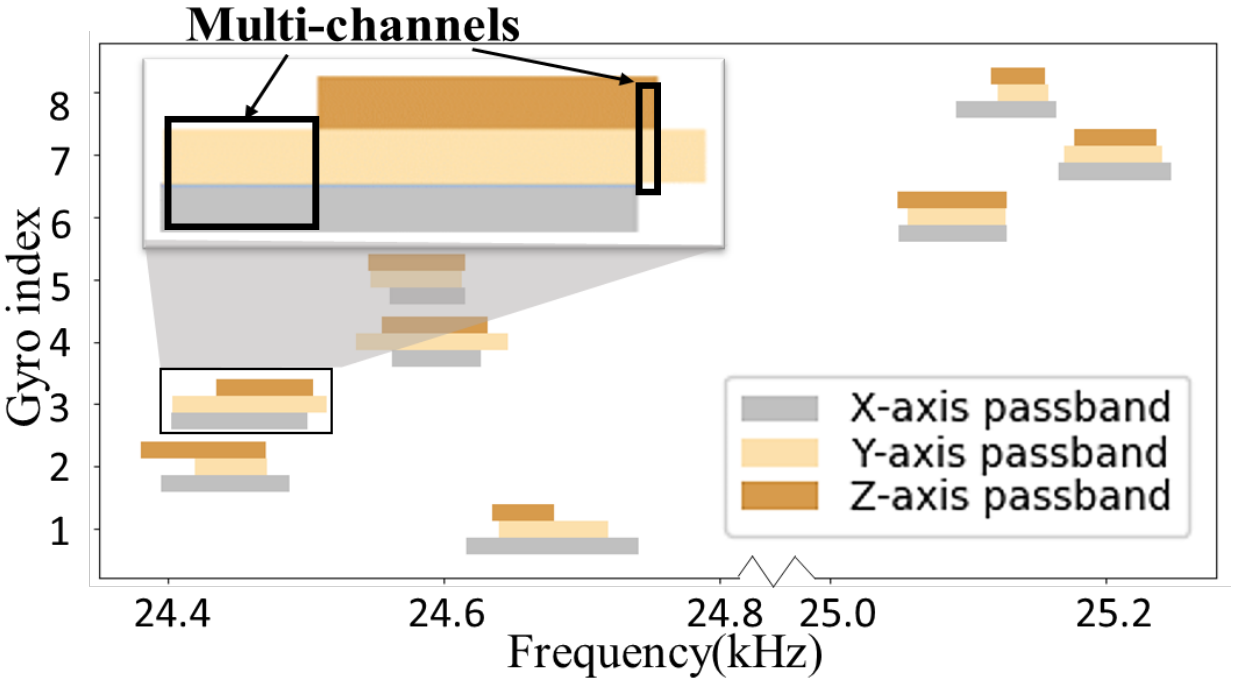


An example of transmission via *Deaf-Aid*



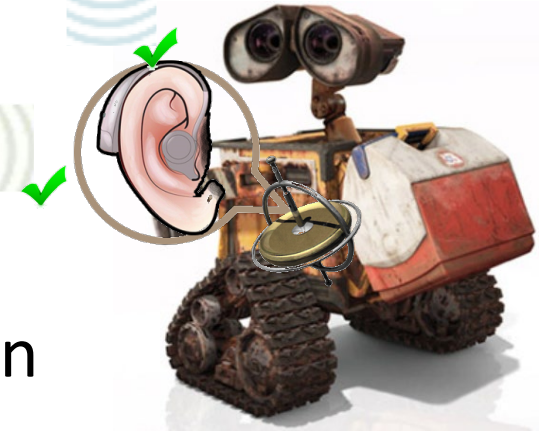
Signals are received by gyroscope!

Multi-channel Support



Keep secret!

What is your mission?



Deaf-Aid supports simultaneous communication on multiple channels, even from two transmitters.

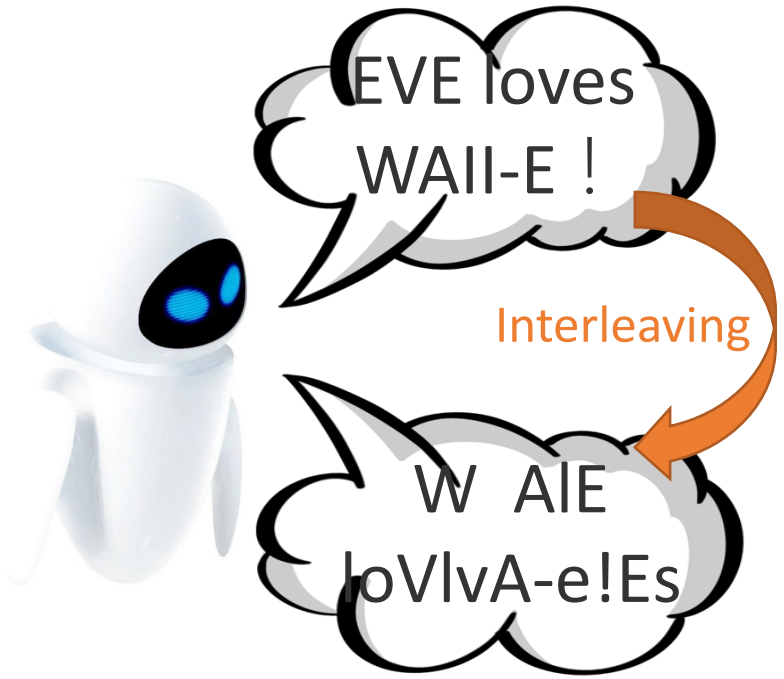
System Overview

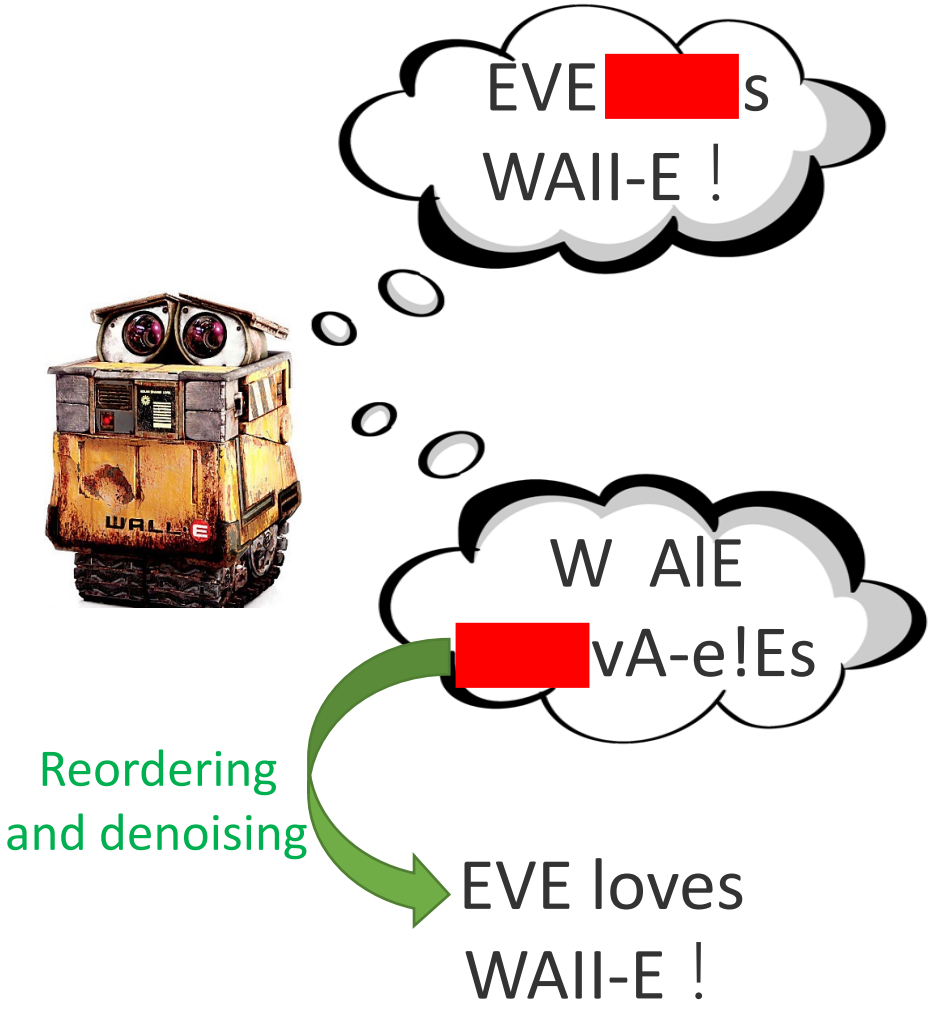
1. How to identify the receiver?

2. How to ensure high-quality communication?

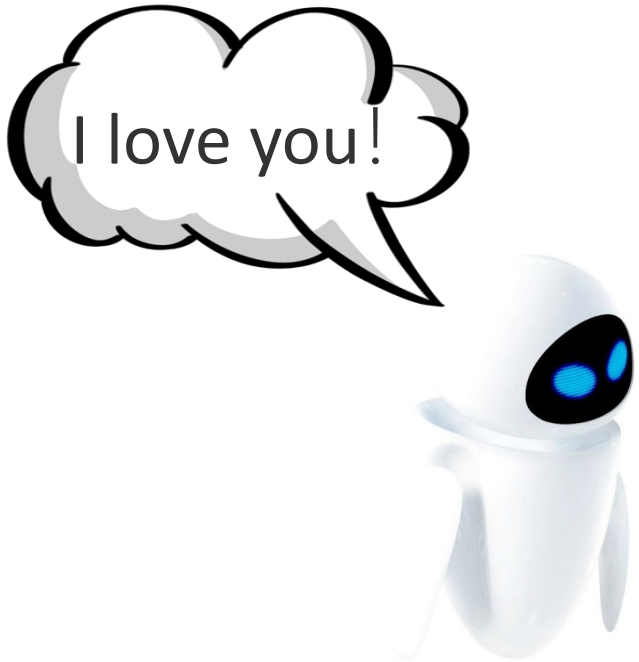
3. How to suppress motion influence?

Line-of-Sight Blocking





Transmitter Motion



A global threshold

I love you!

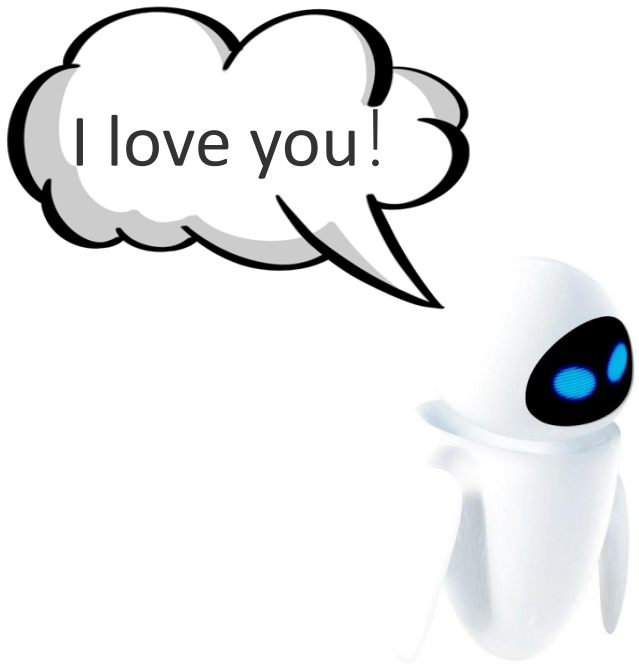
I ve ou!

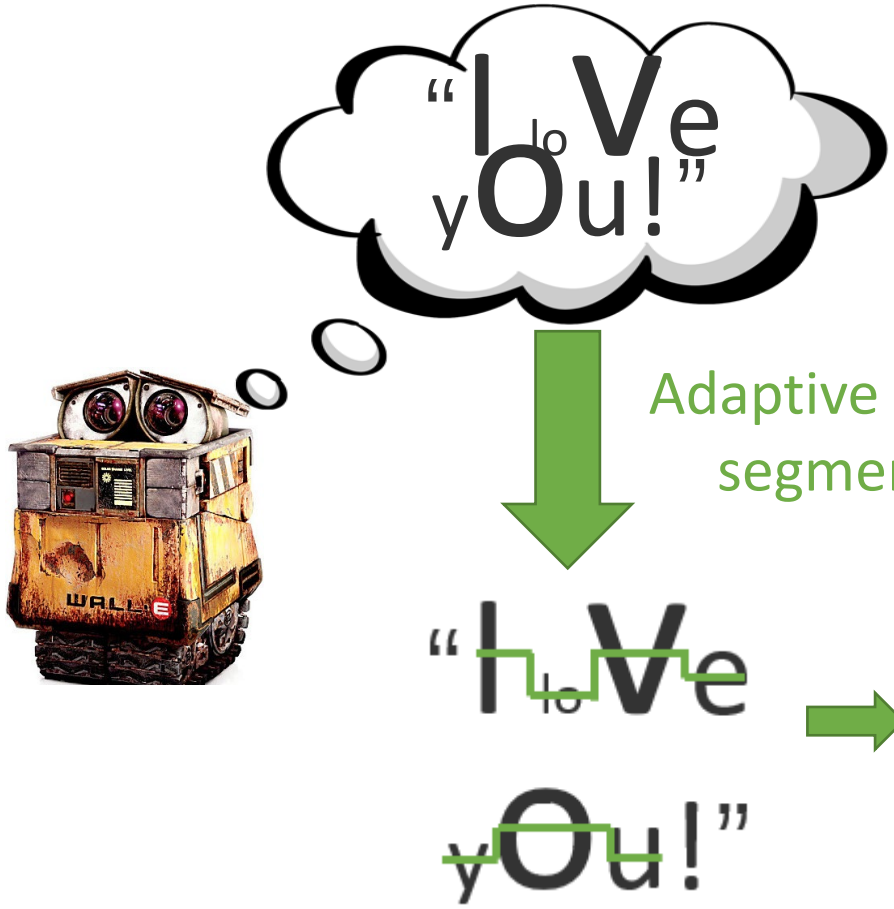
or

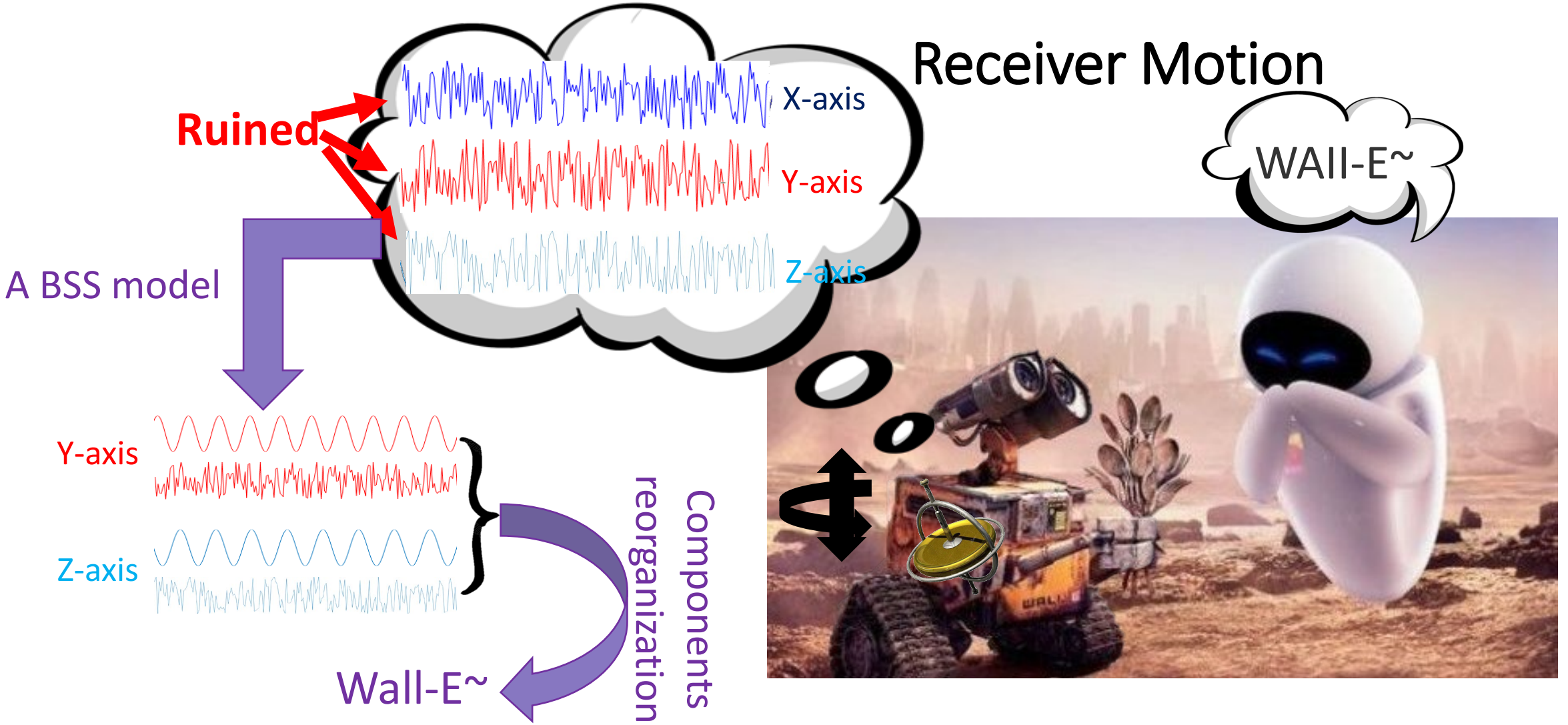
I love you!

In lovnen yonun!

Transmitter Motion

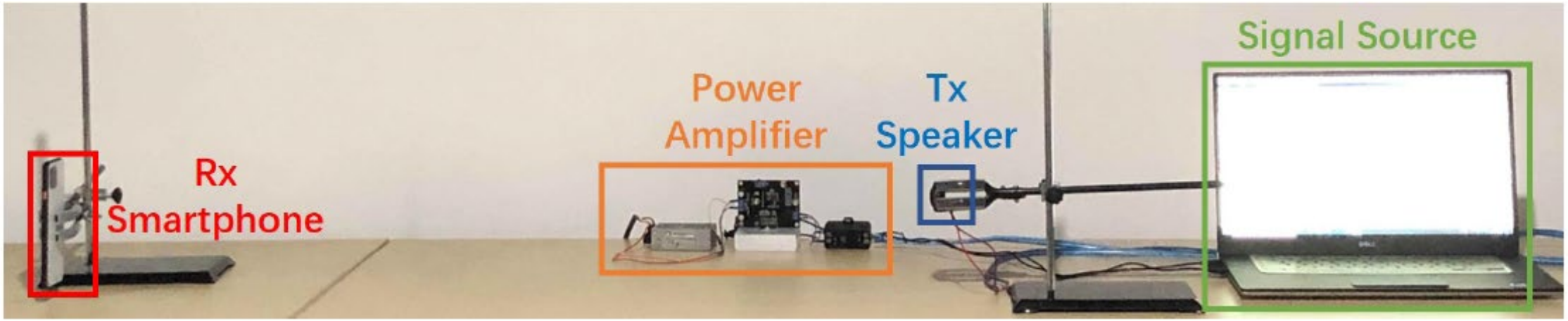




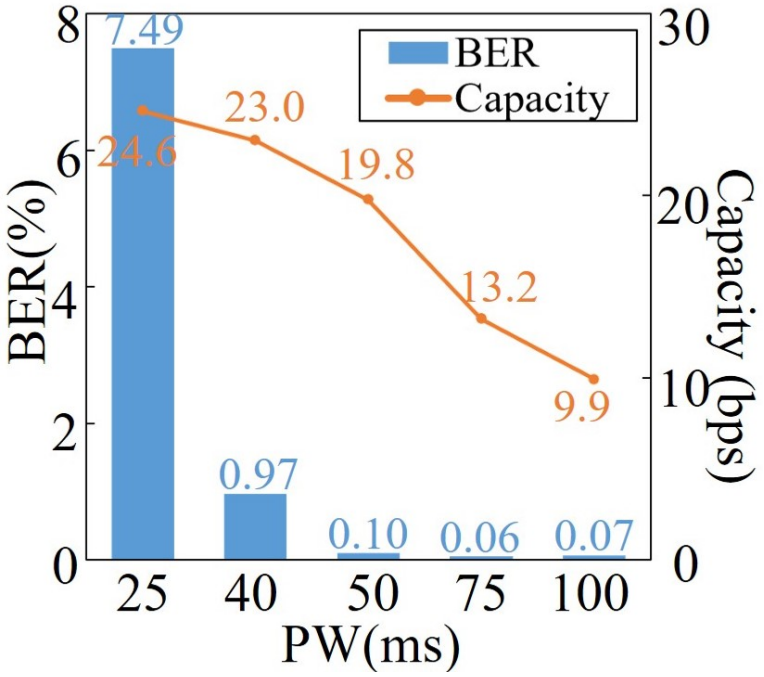


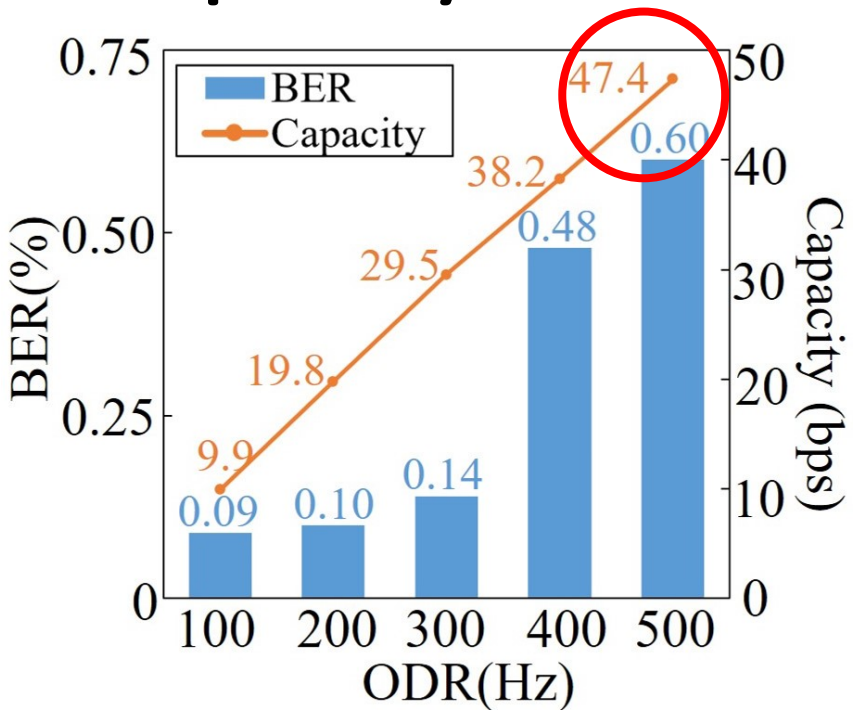
Deaf-Aid manages to be robust against movements.

Experimental Setup



Transmission Capacity

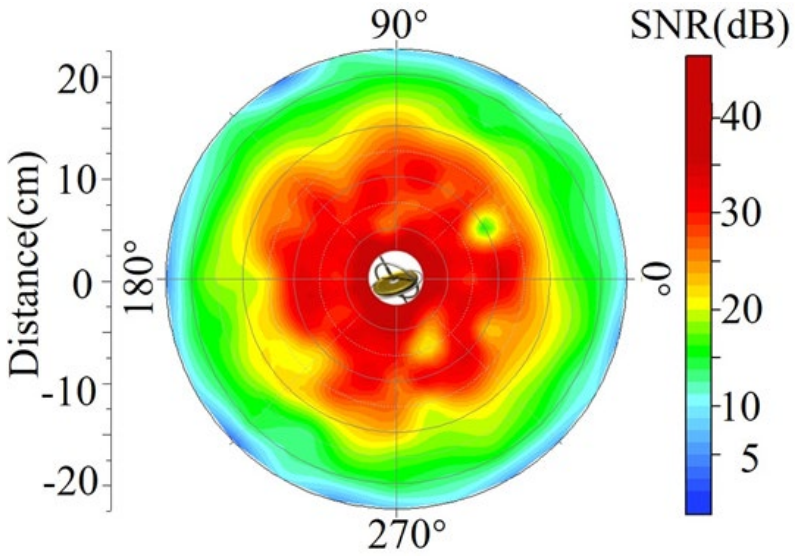


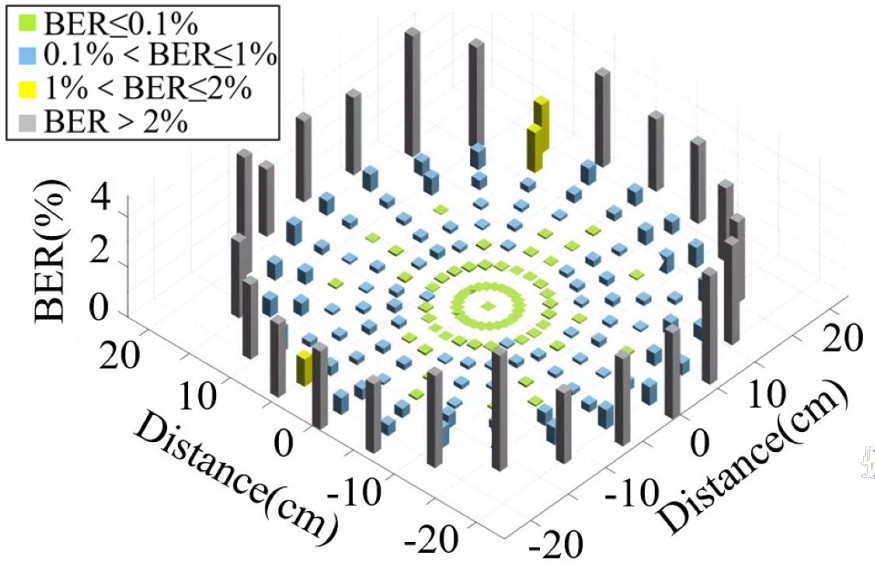


Error-free and high-speed communication

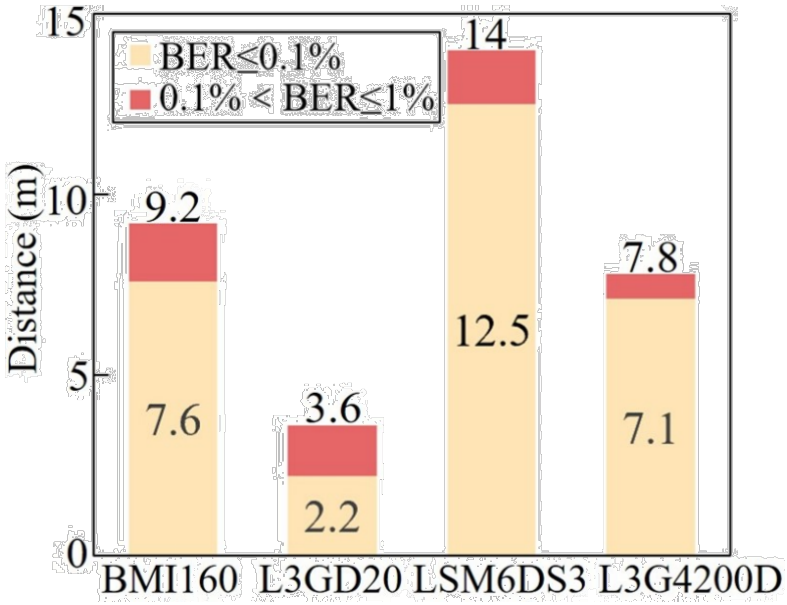
- Channel capacity reaches 47bps
- BER remains a low level within 0.6%
- *Deaf-Aid* is competent for the different requirements of transmission speed and tolerance of error flexibly in various occasions.

Orientation and Distance



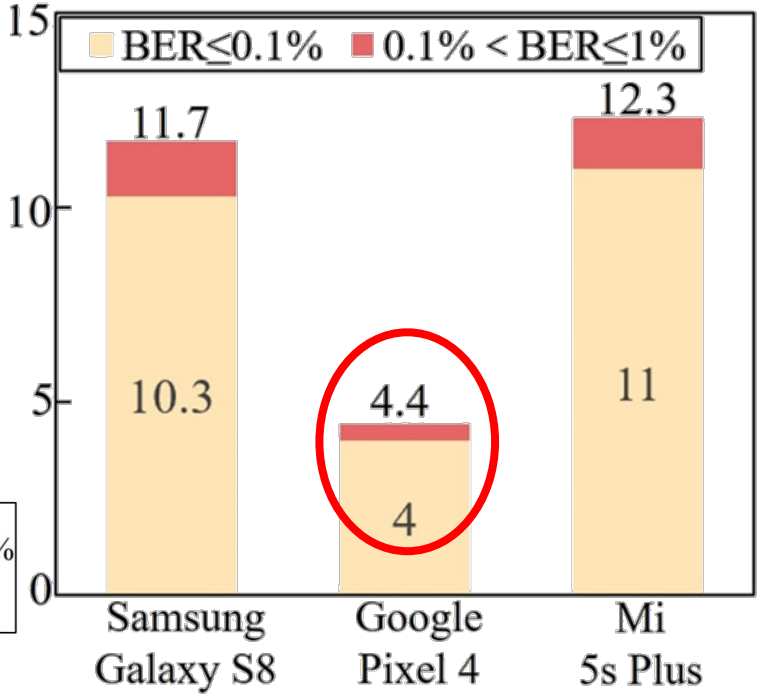


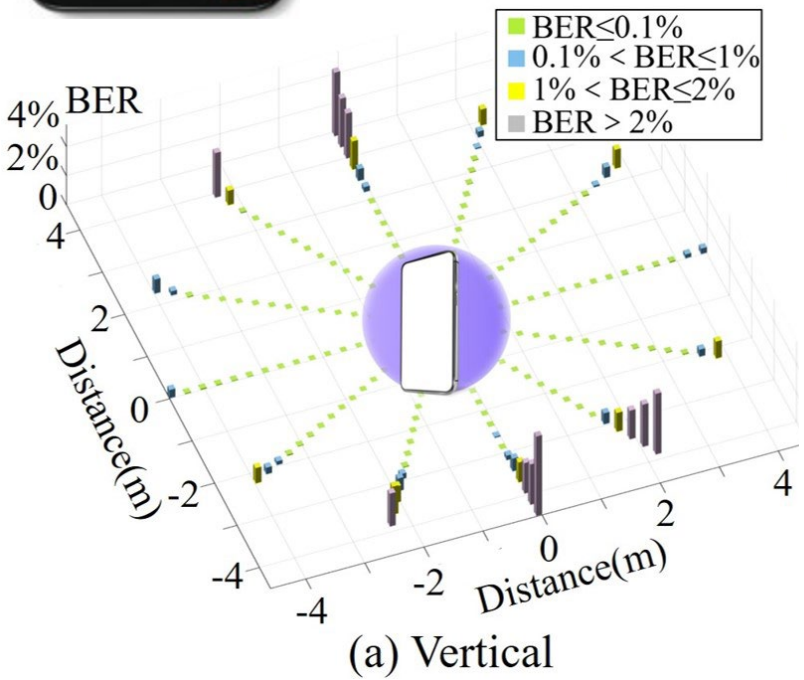
- Scarce constraints on the orientation
- The distance is extended up to 14m



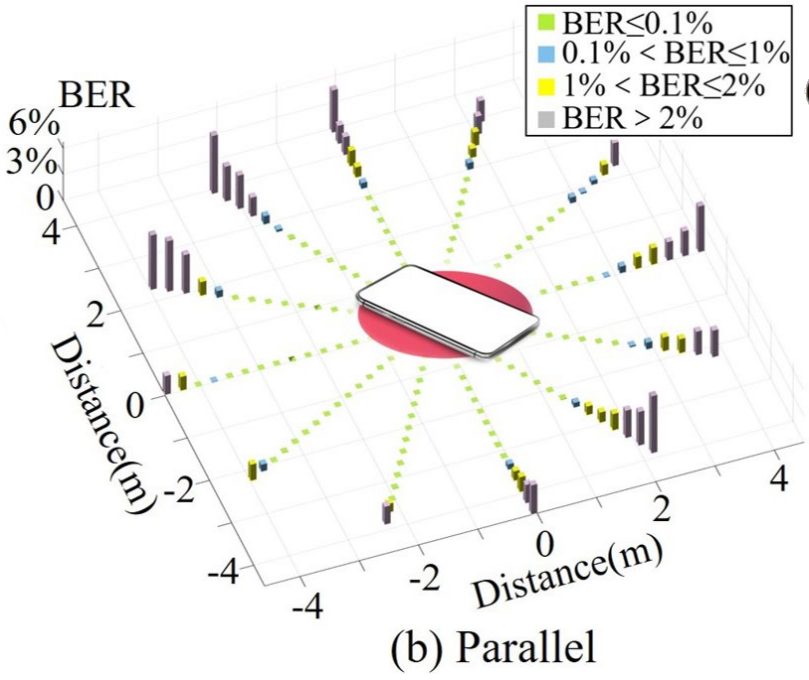
Smartphone Prototype

- We rotate a speaker around the fixed phone
- Two different position
- Scarce constraints on the orientation



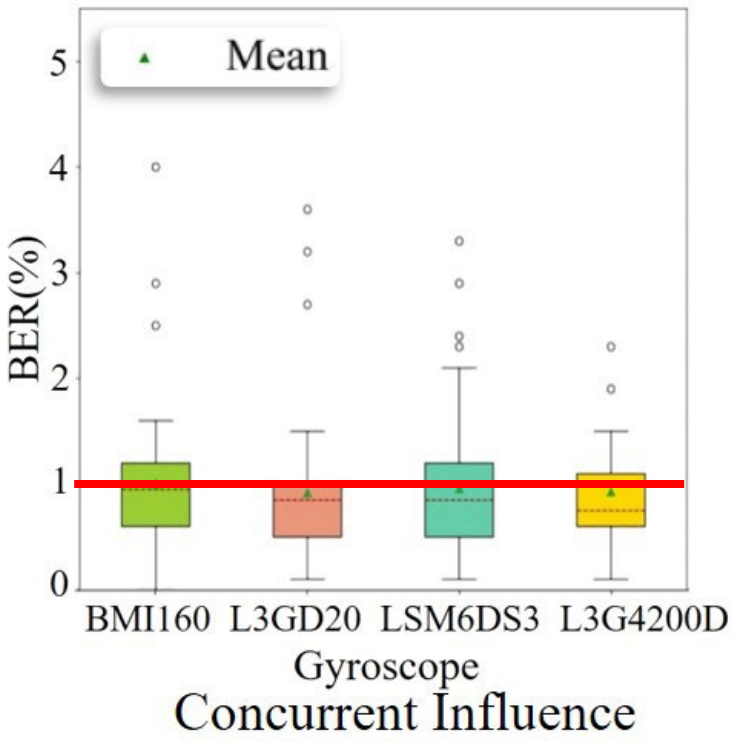


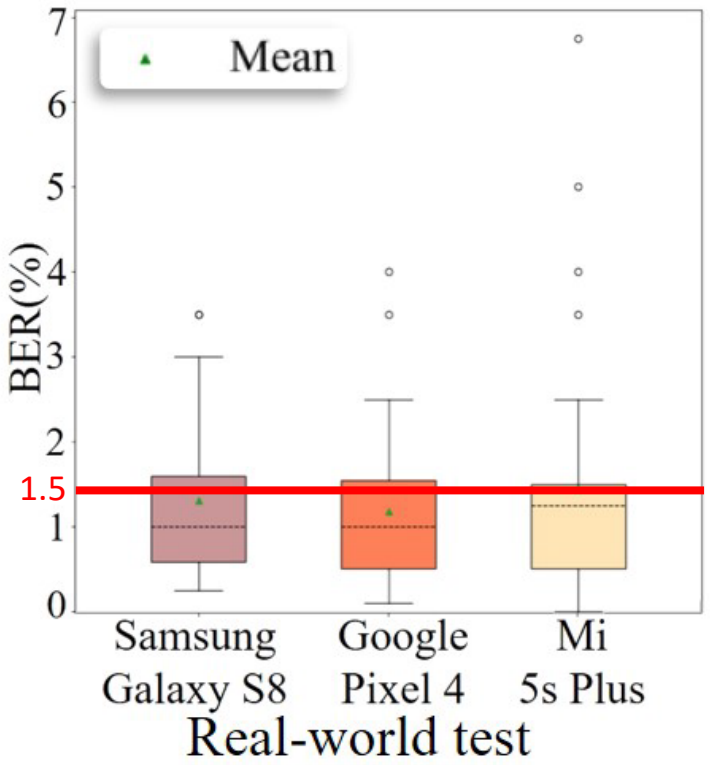
(a) Vertical



(b) Parallel

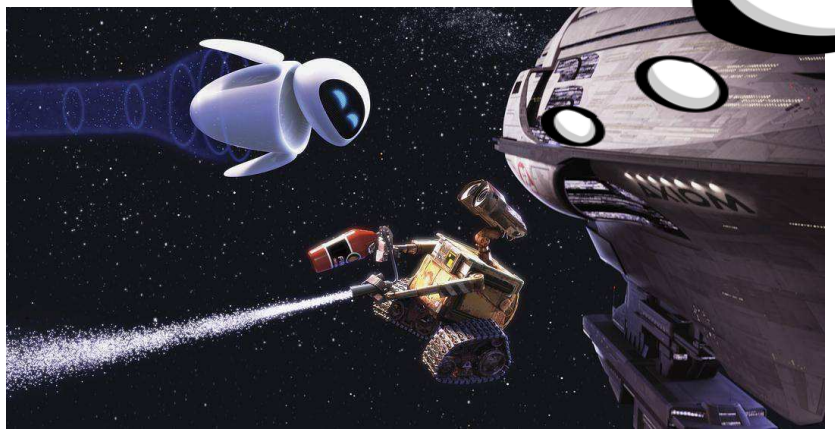
The communication distance can reach up to 12 meters among realistic devices.





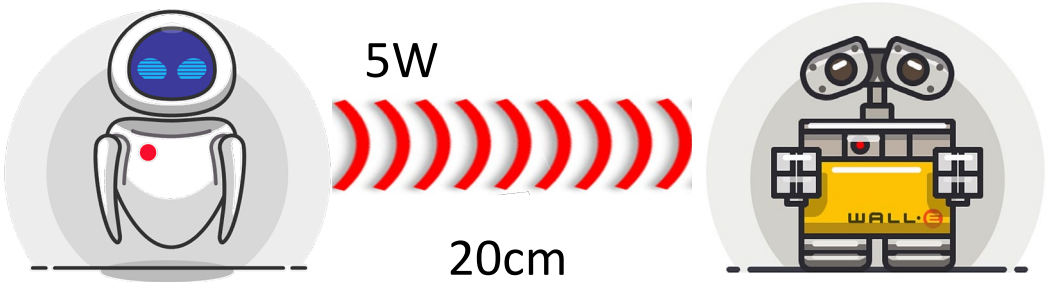
Robust to movement

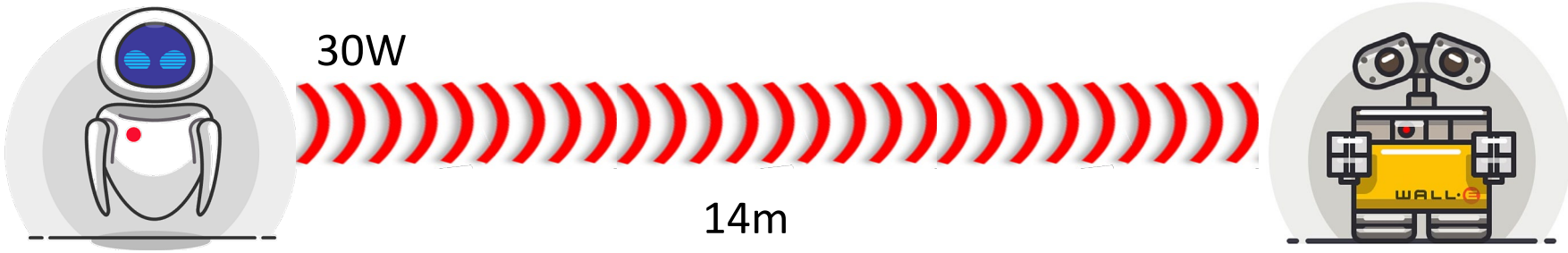
Motion Influence

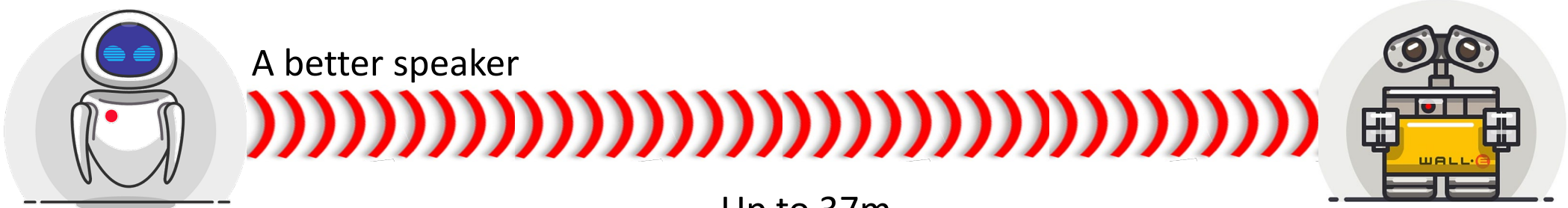


	Ripple [RGC15]	Ripple II [RC16]	BitWhisper [GMME15]	Dhwani [NCPV13]	Deaf-Aid
Speed	200bps	30kbps	1-8 bits per hour	2.4kbps	47bps
Accuracy	BER<1.7%	SNR>15db	Not evaluate	Accuracy>95%	BER<0.6%
Distance	6 inches	Touch based	40cm	10cm	14m
Free Placement	✗	✗	✗	✓	✓
No need for Peripheral	✓	✓	✓	✗	✓
Motion Robustness	✗	✗	✗	✓	✓
Automatic Identification	✗	✗	✗	✗	✓

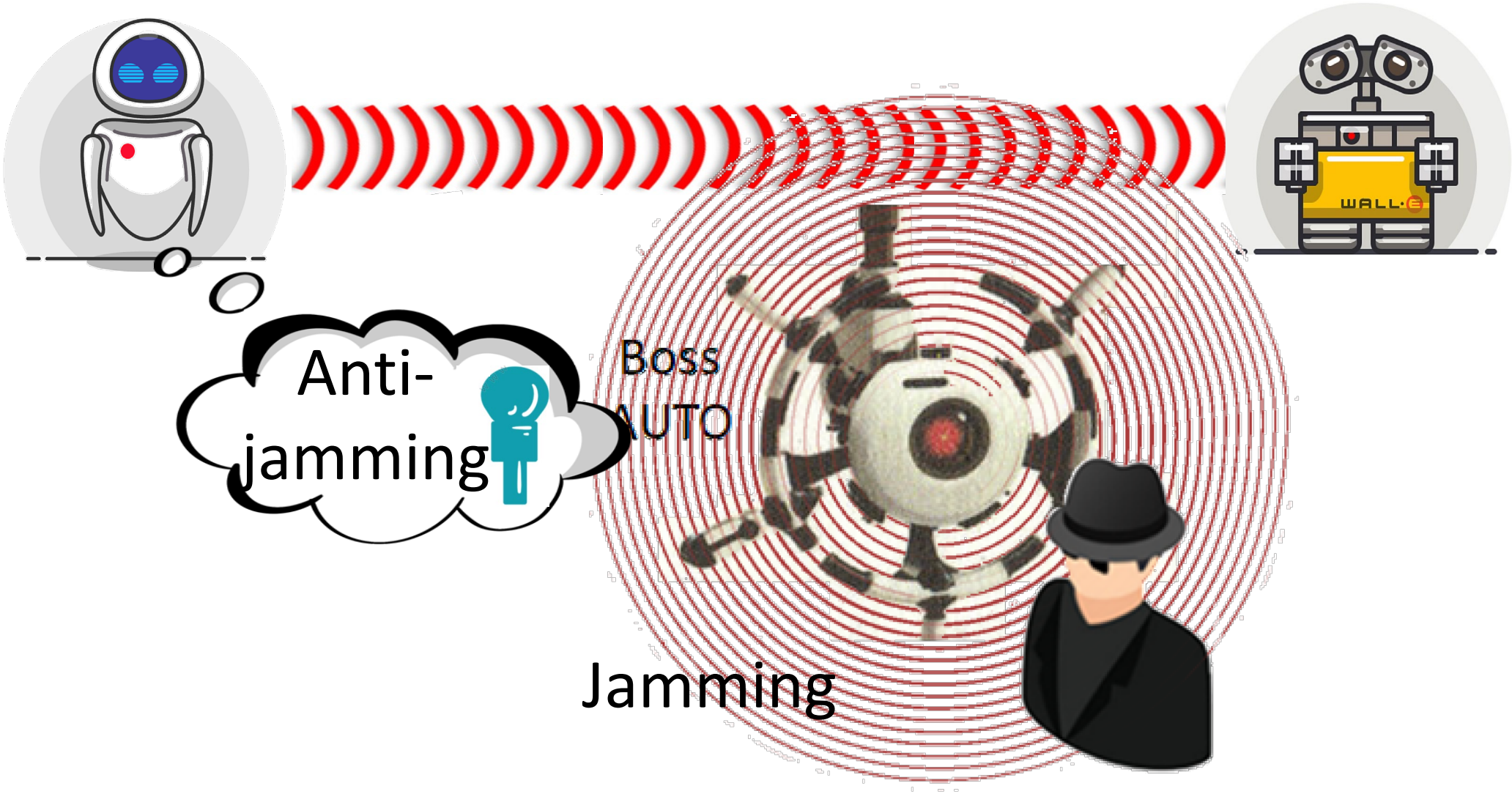
Implementation Consideration



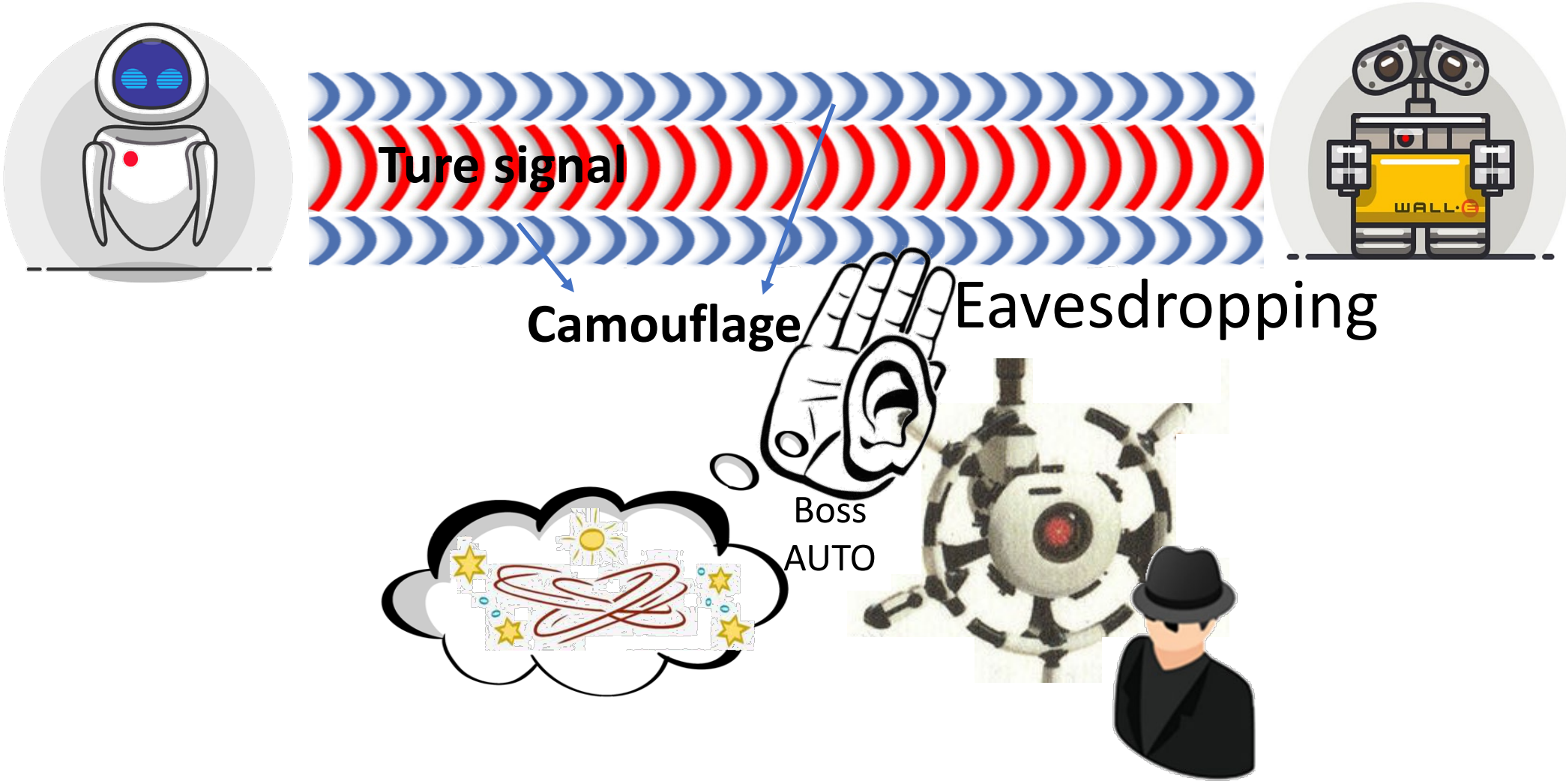




Security



Security



Conclusions

- We build the speaker-to-gyroscope channel, *Deaf-Aid,* for protocol-independent mobile IoT communication.
- We analyze the inter-axes relationship in a gyroscope under resonance.
- *Deaf-Aid* leverages the diversity of resonant passband of gyroscope as device fingerprint to identify receivers.

Thank you!

Contact

Ming Gao	minggao5@acm.org
Feng Lin	flin@zju.edu.cn
Weiye Xu	xuweiye@zju.edu.cn
Muertikepu Nuermaimaiti	murtakip@zju.edu.cn
Jinsong Han	hanjinsong@zju.edu.cn
Wenyao Xu	wenyaoxu@buffalo.edu
Kui Ren	kuiren@zju.edu.cn

Reference

- [RC16] N. Roy and R. R. Choudhury. 2016. Ripple II: Faster Communication through Physical Vibration. In *13th USENIX Symposium on Networked Systems Design and Implementation.*

- [RGC15] N. Roy, M. Gowda, and R. R. Choudhury. 2015. Ripple: Communicating through Physical Vibration. In *12th USENIX Symposium on Networked Systems Design and Implementation*.

- [GMME15] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici. 2015. BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. *In IEEE 28th Computer Security Foundations Symposium.*

- [NCPV13] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan. 2013. Dhwani: secure peer-to-peer acoustic NFC. *ACM SIGCOMM Computer Communication Review 43*.4 (2013), 63¨C74.