ECE 598HH: Advanced Wireless Networks and Sensing Systems

Lecture 19: Full Duplex Radios

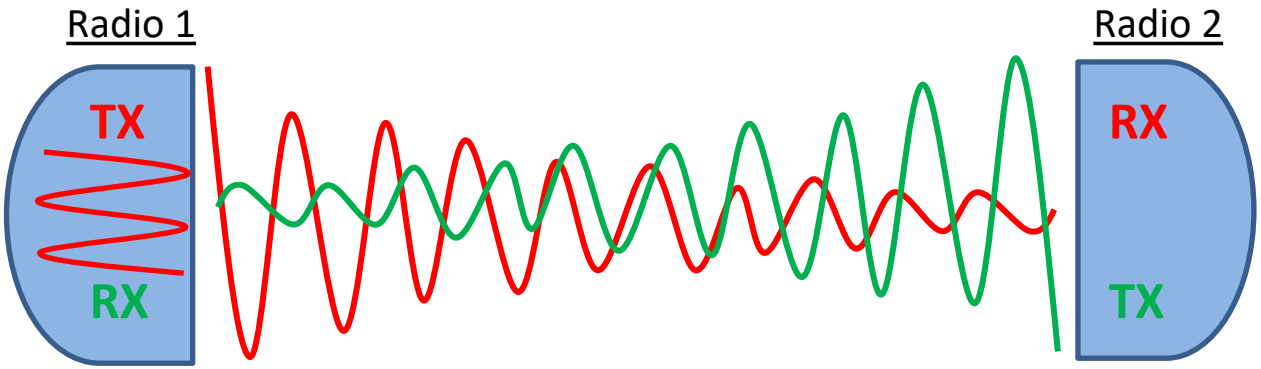
Haitham Hassanieh

*These slides are courtesy of Dinesh Bharadia (UCSD) & Yunfei Ma (MIT)

"It is generally not possible for radios to receive and transmit on the same frequency band because of the interference that results."

- Andrea Goldsmith, "Wireless Communications," Cambridge Press, 2005.

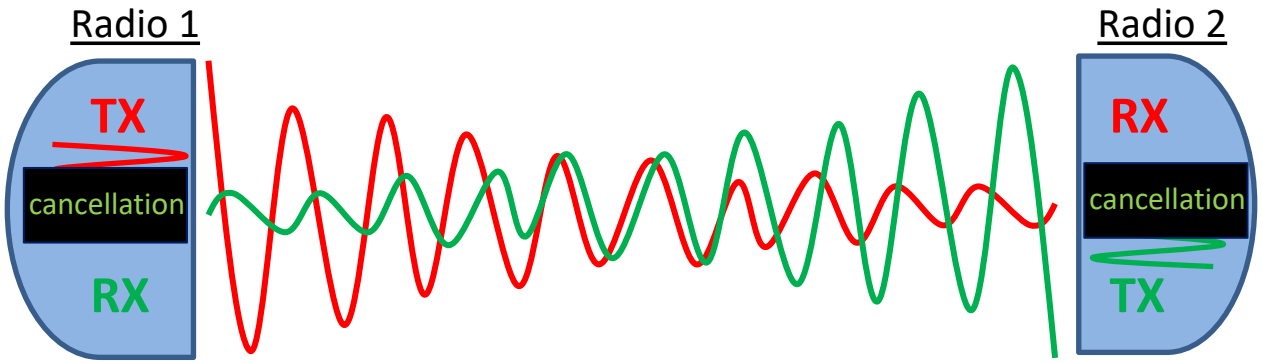
Why Aren't Radios Today Full Duplex?



Self

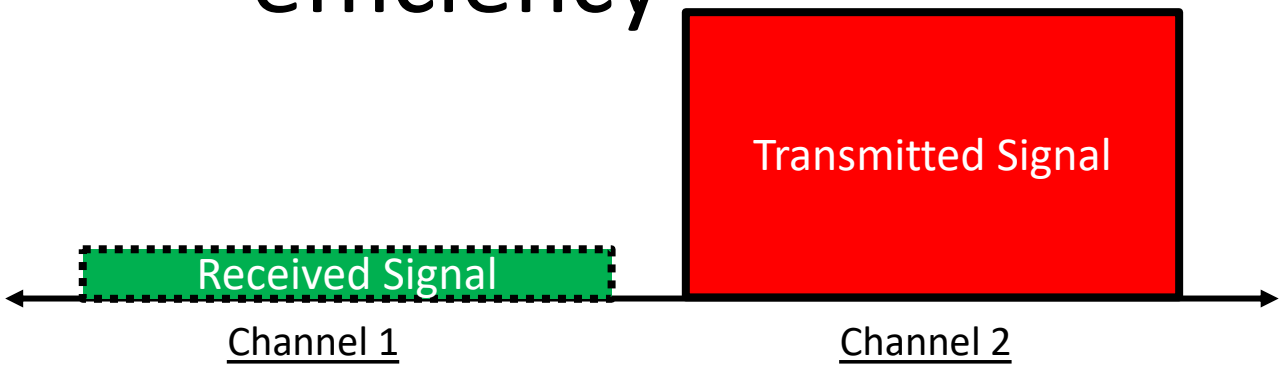
ger

With self-interference cancellation, radios can transmit and receive on the same channel!

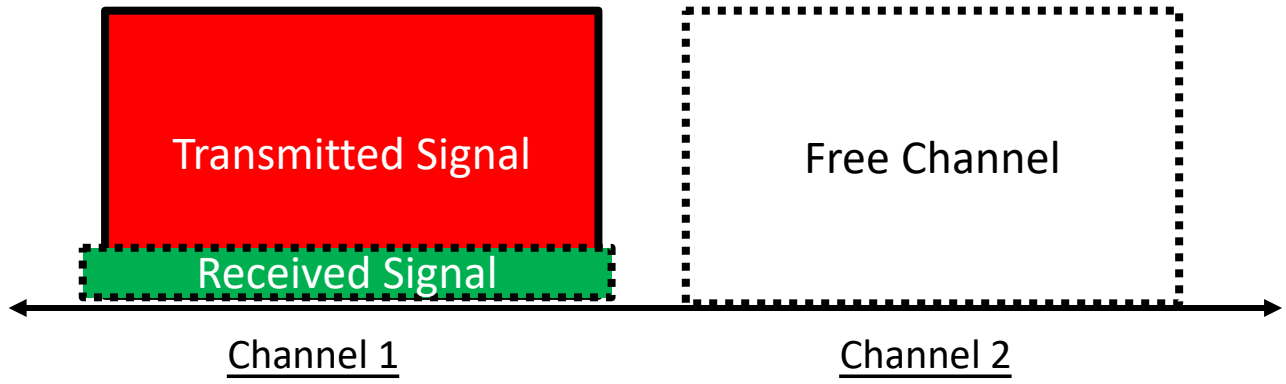


Self-Interference Cancellation enables full-duplex, doubles spectral efficiency

LTE requires paired frequencies

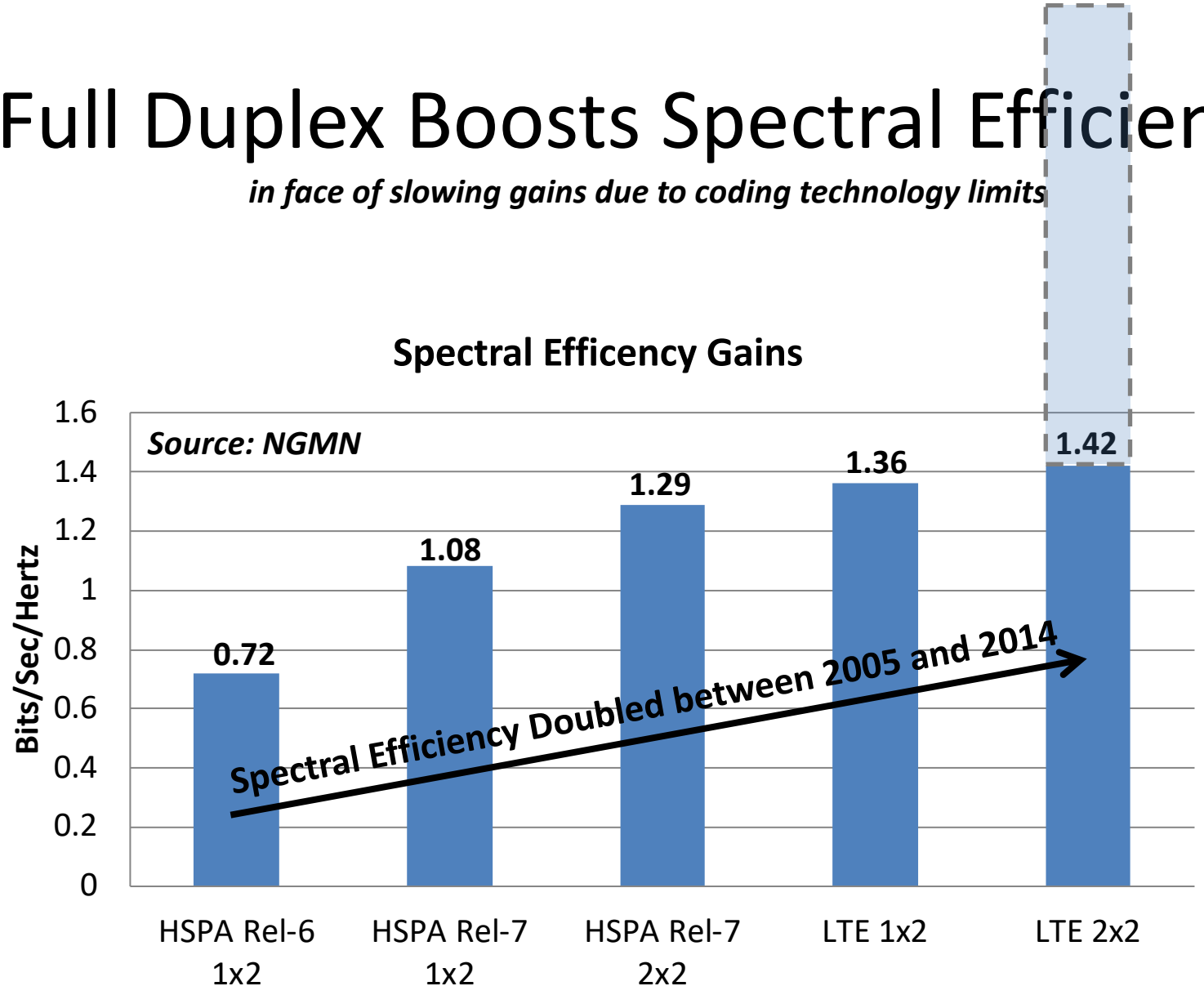


Full-duplex uses single frequency for same performance



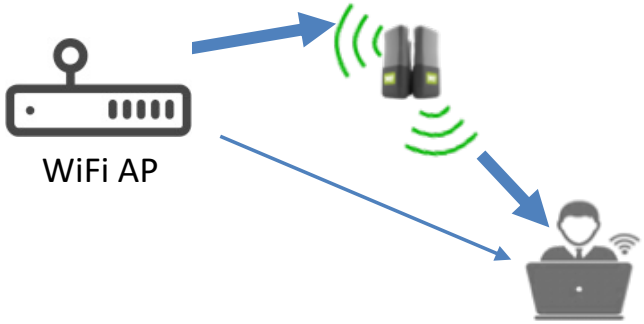
Full Duplex Boosts Spectral Efficiency

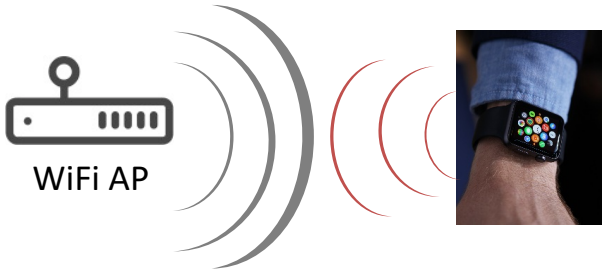
in face of slowing gains due to coding technology limits

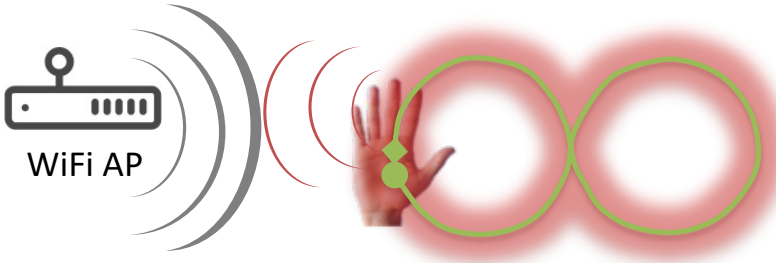


Applications of full duplex radios:

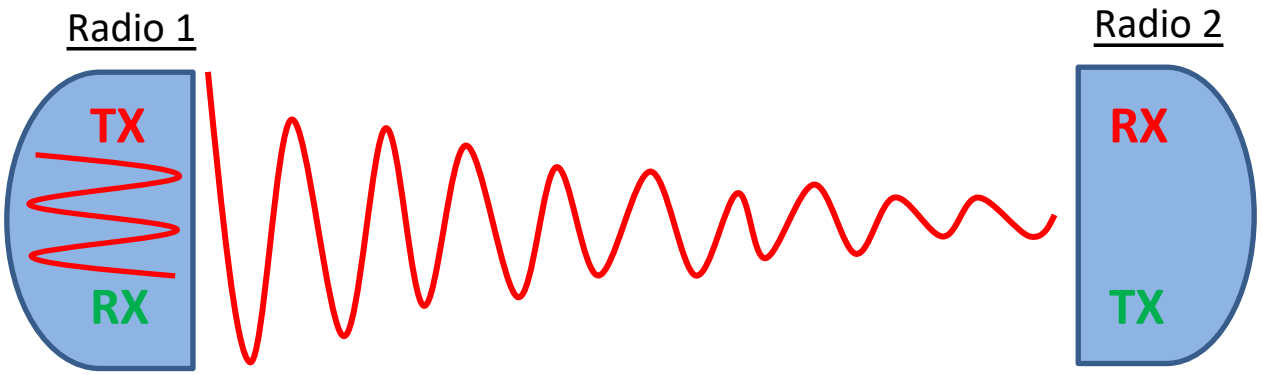
- TX/RX on same time same channel
  → Double Spectral Efficiency!
- Extend range with full duplex relays
- WiFi Backscatter
- Better MAC: CSMA/CD in wireless
- Motion tracking & imaging in WiFi
- Security: Friendly Jamming







Motion tracking & Imaging

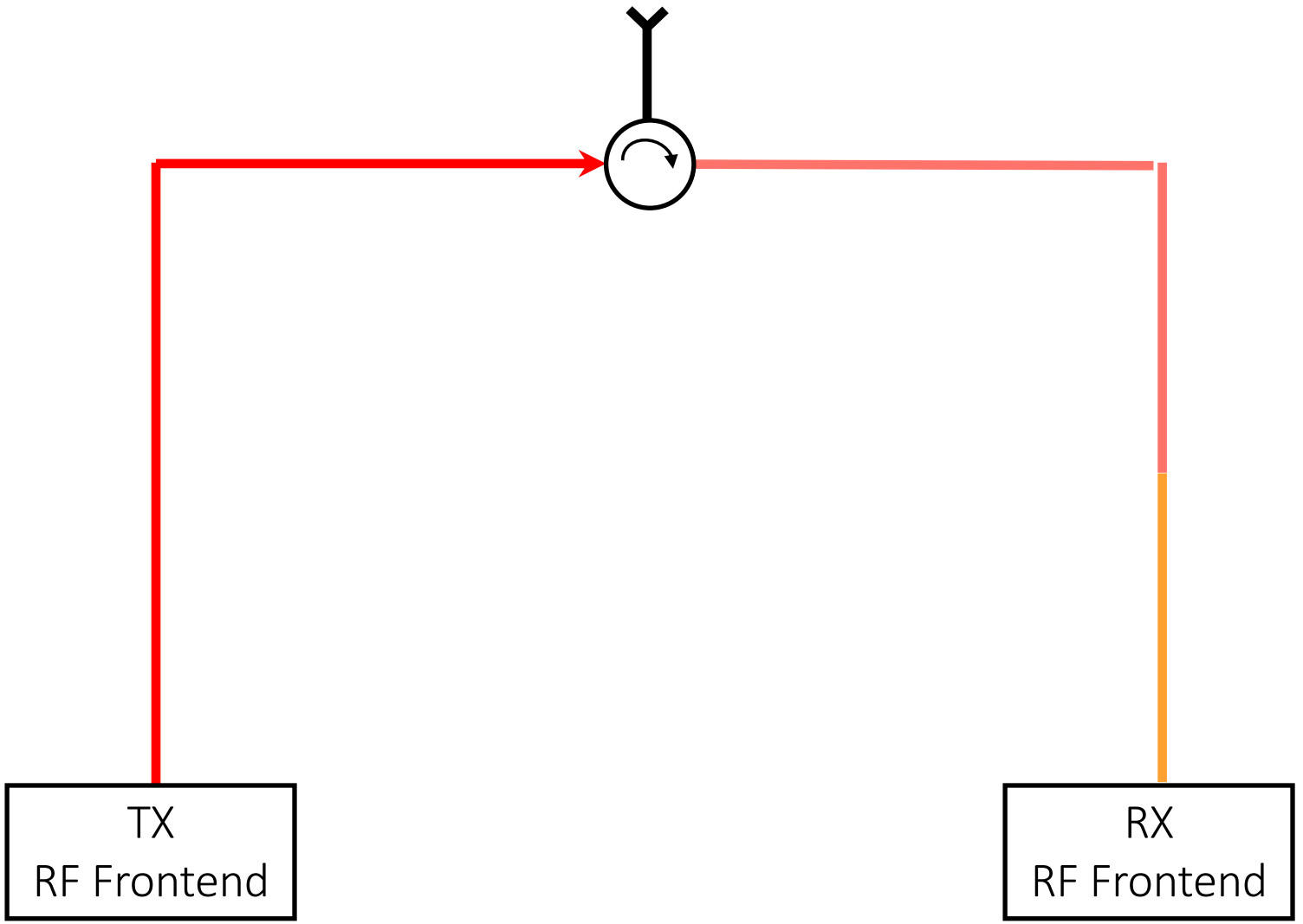


Isn’t this easy to solve?

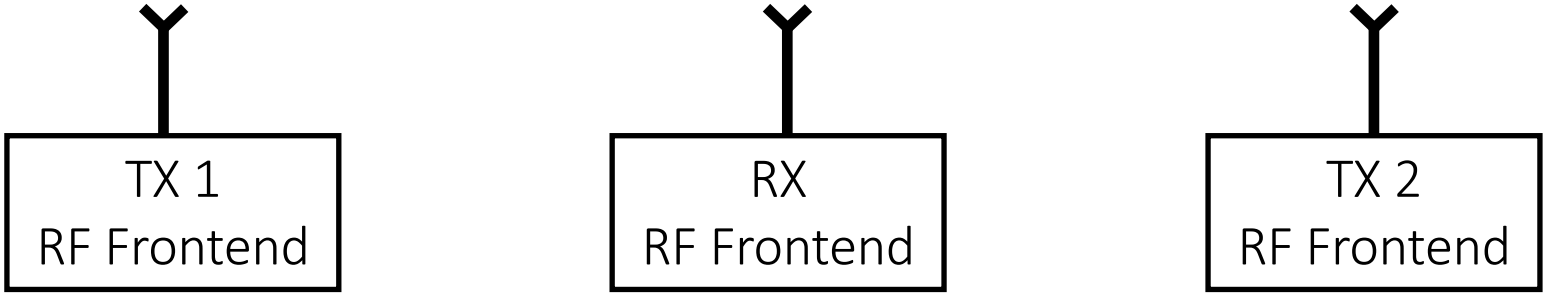
After all we know the interfering signal, why can’t we just “subtract” it?

Solution 1: RFID Readers Already Do It!

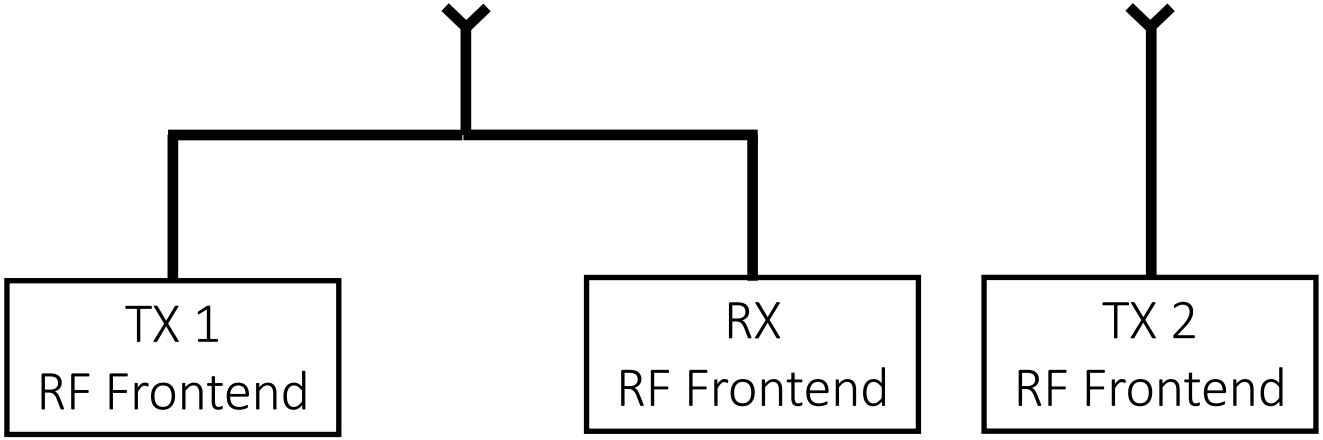
Solution 2: Circulator



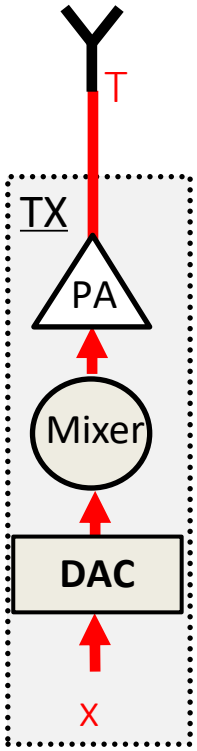
Solution 3: Nulling by Antenna Placement.



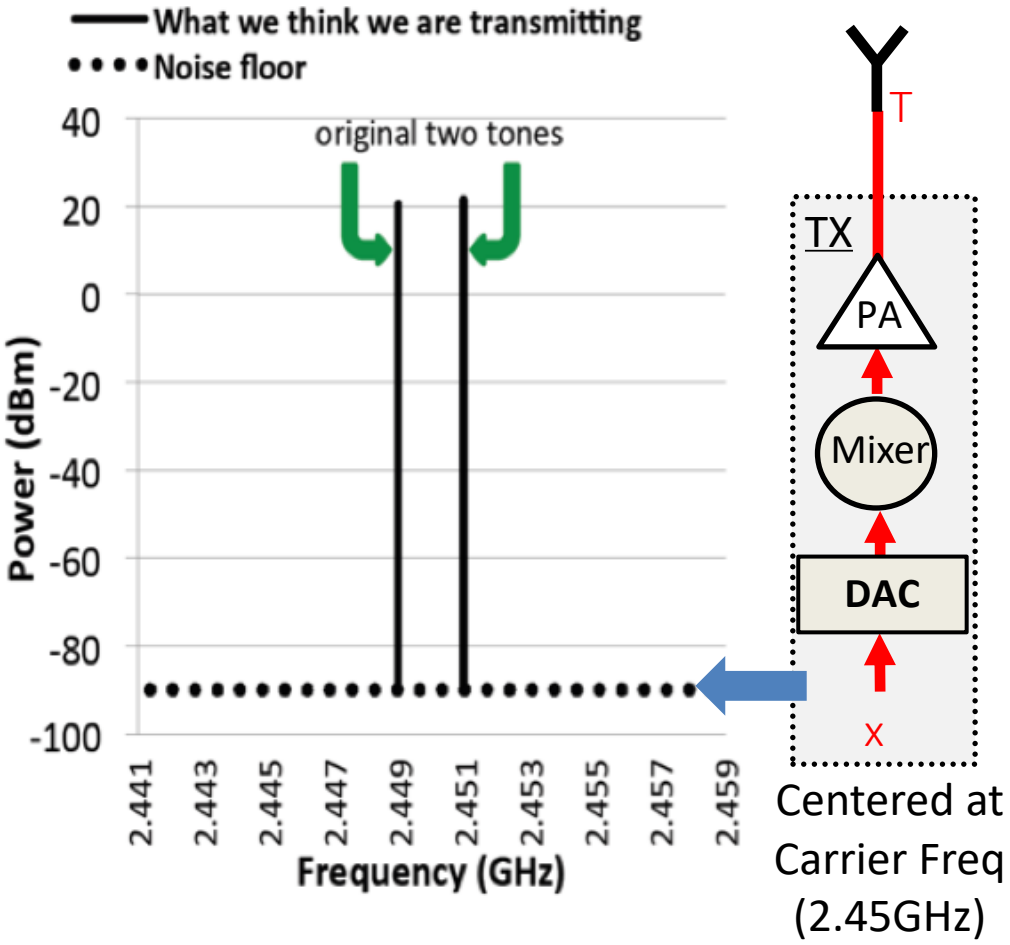
Solution 4: Nulling in hardware



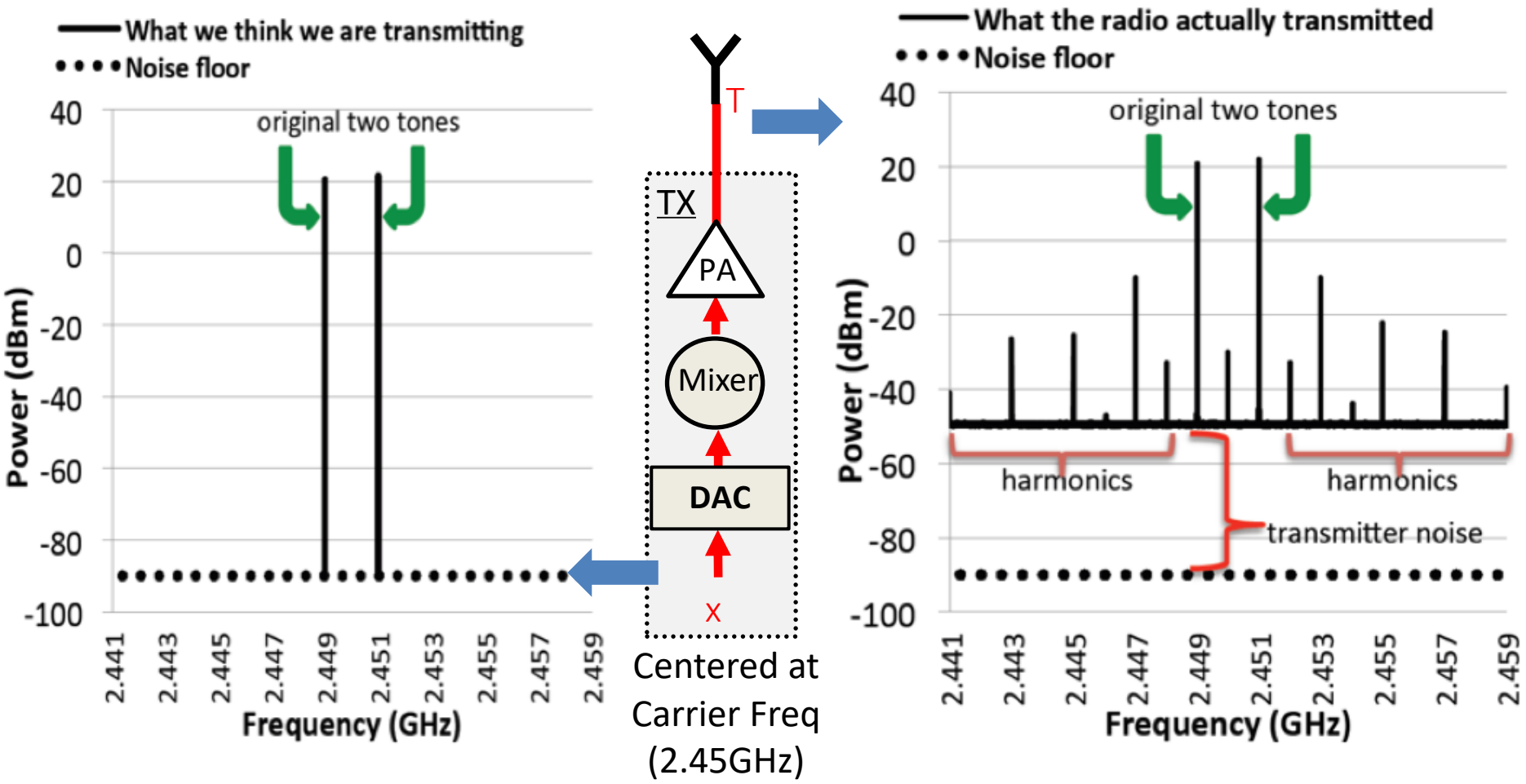
Do we know what we are transmitting?



Do we know what we are transmitting?



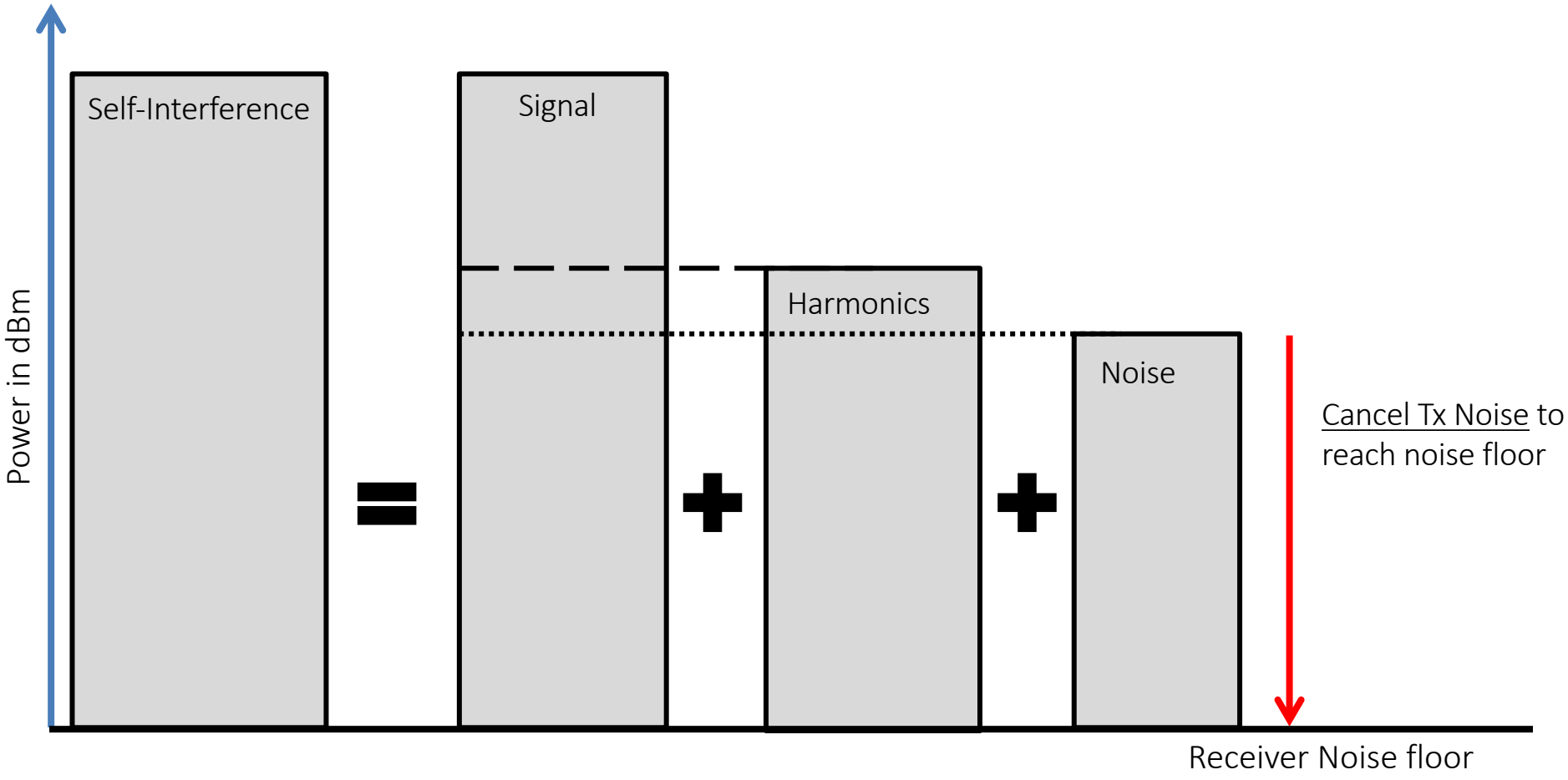
Do we know what we are transmitting?



Transmitted Signal = Signal + Harmonics + Noise

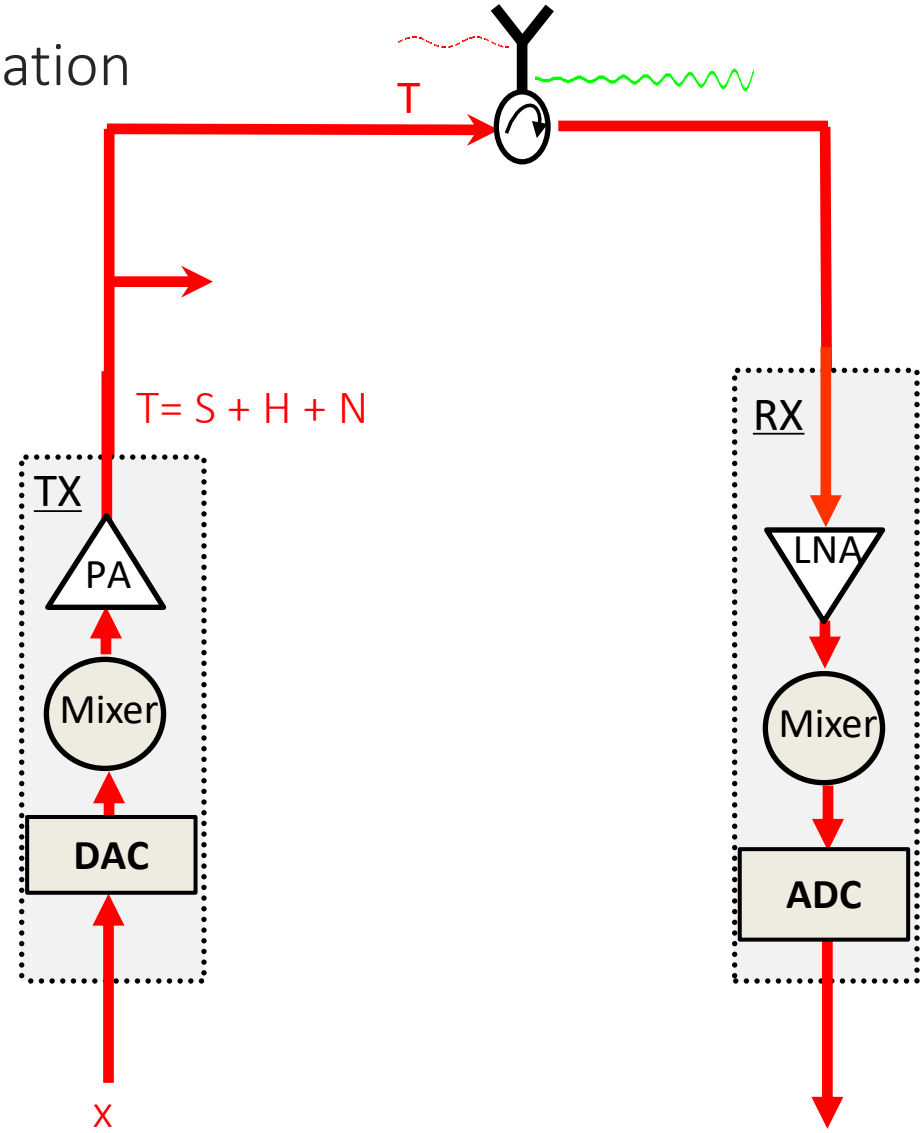
Self-Interference = Signal + Harmonics + Noise

If you were to cancel, how should we cancel?



Solution 5: Analog & Digital Cancellation

Take the copy of the signal and cancel it!

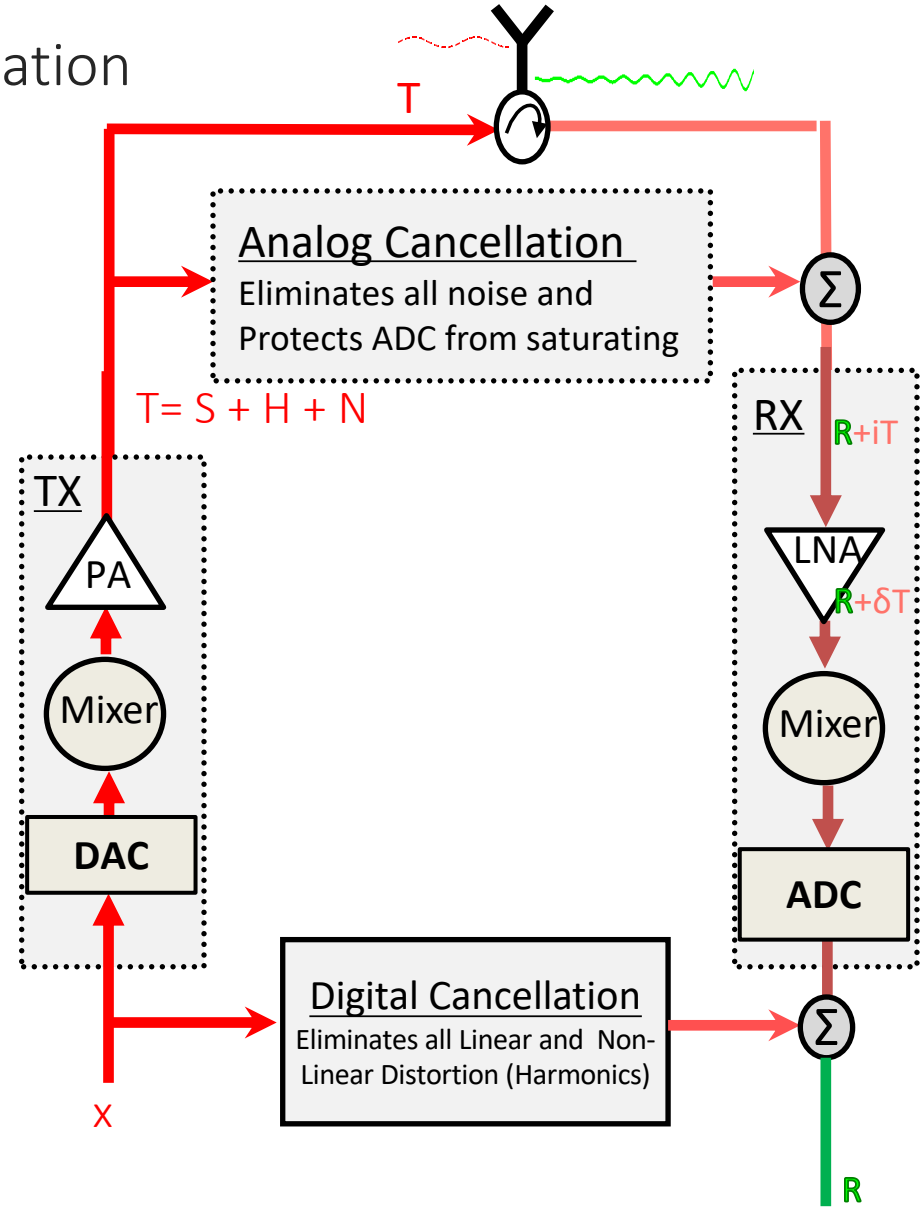


Solution 5: Analog & Digital Cancellation

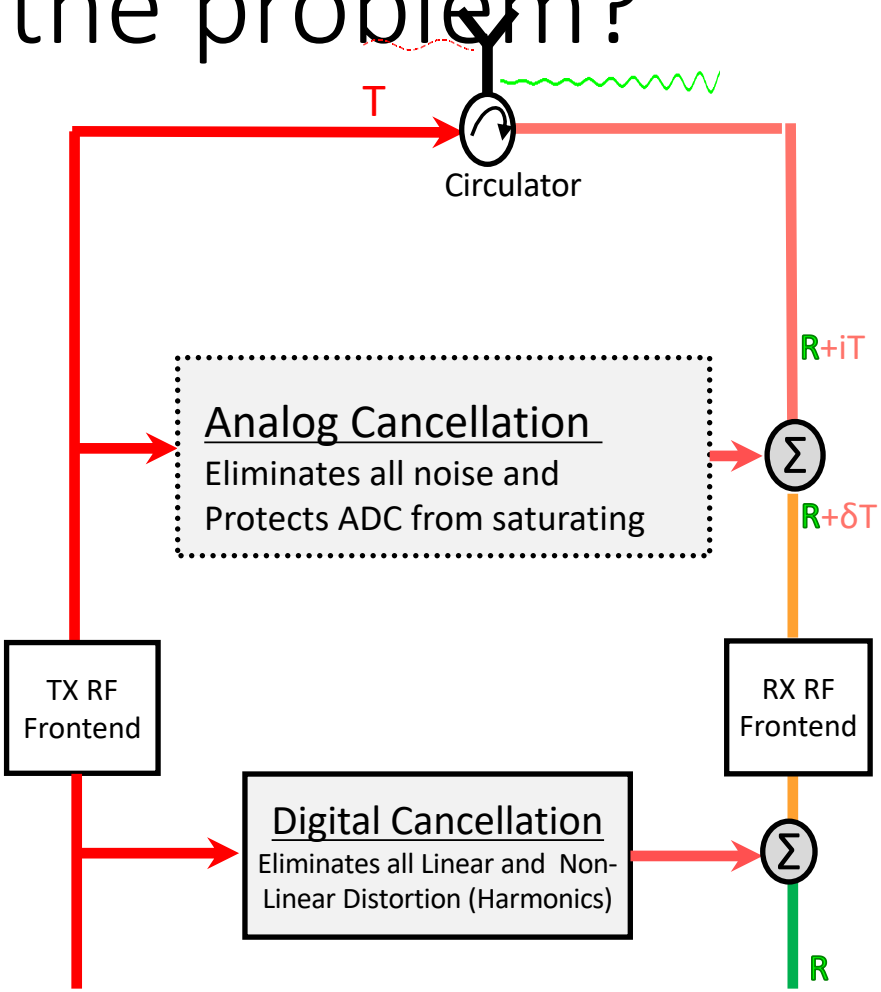
Take the copy of the signal and cancel it!

Analog Cancellation eliminates Noise in analog domain, protect the ADC

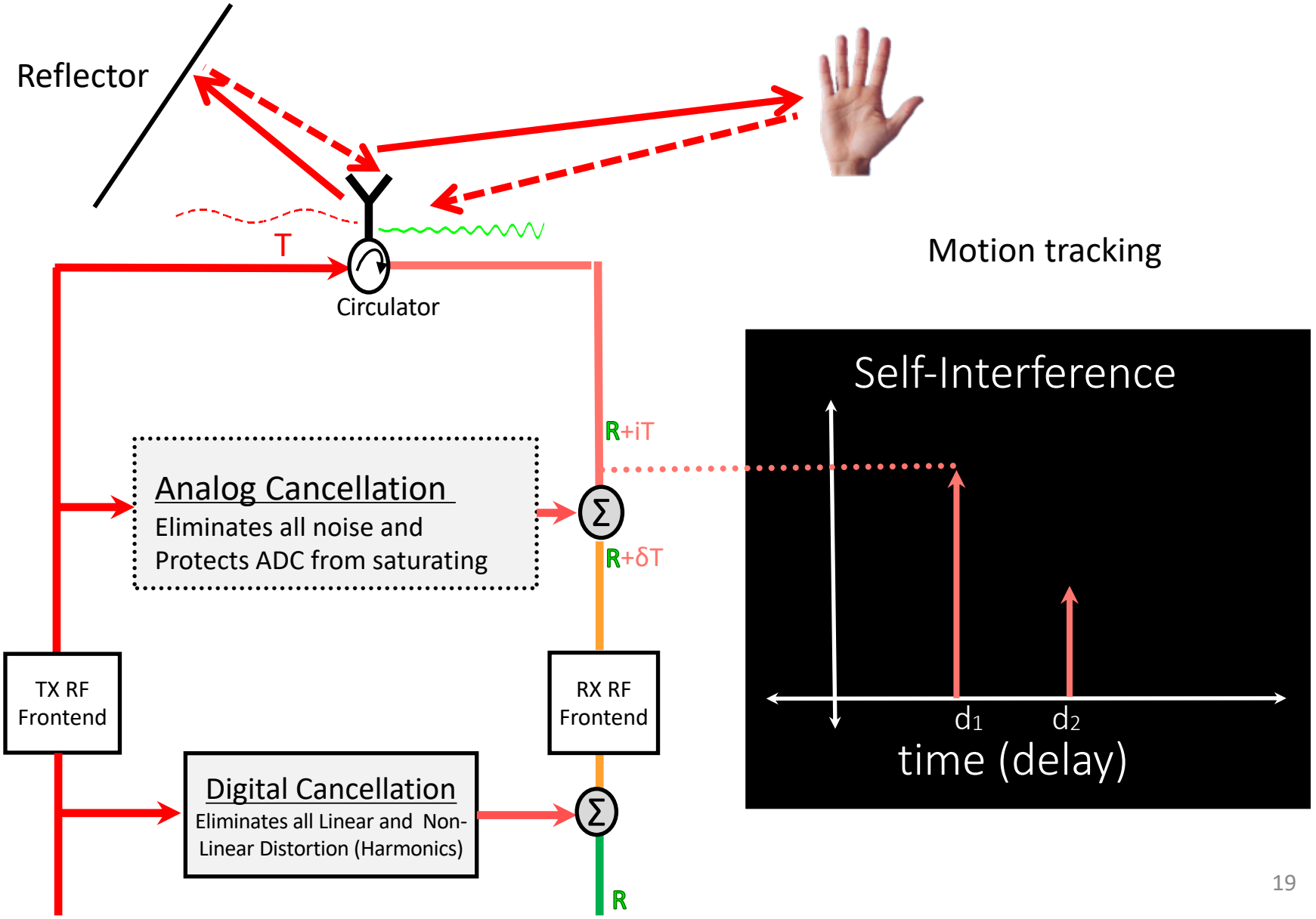
Digital Cancellation eliminates the residual signal and harmonics.



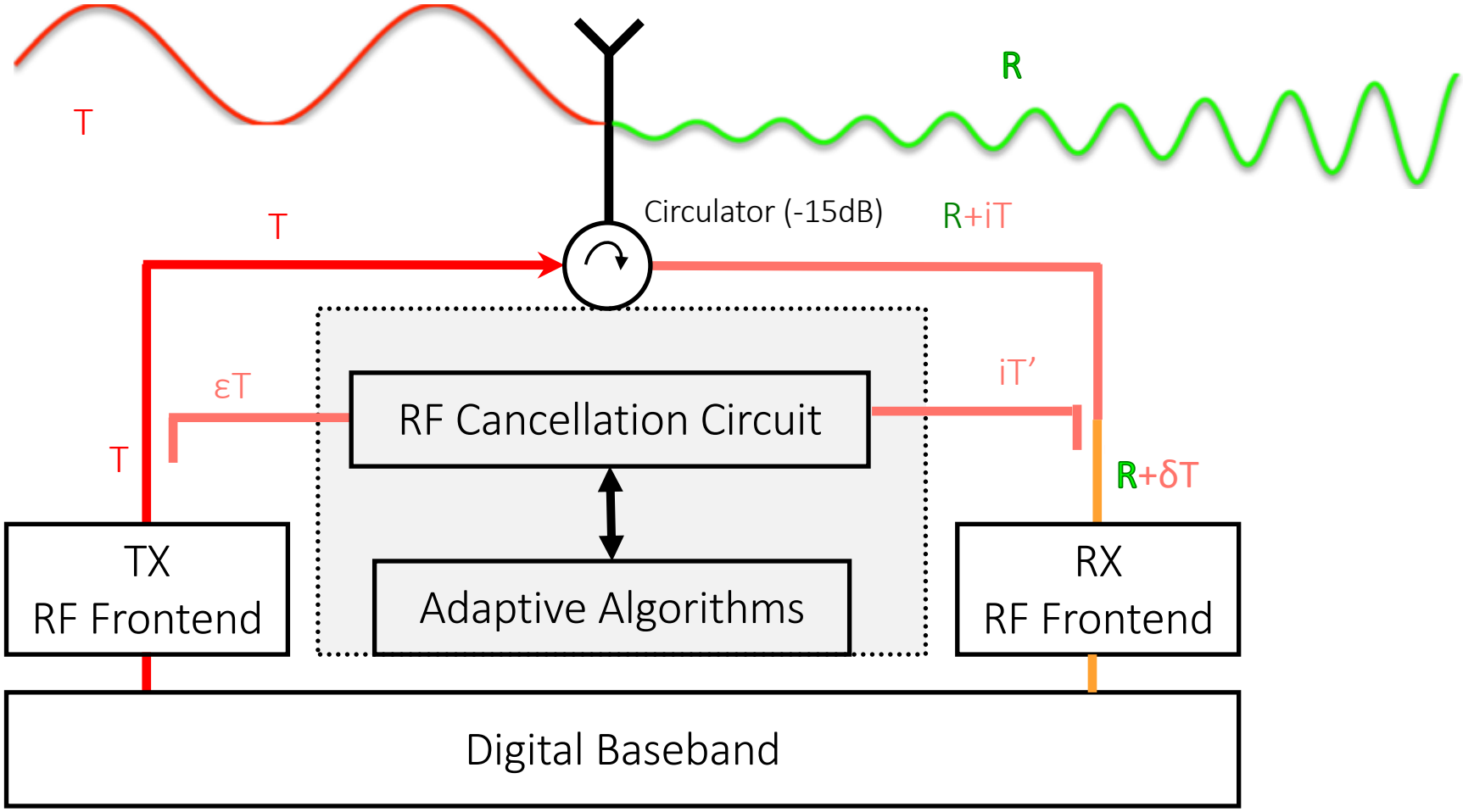
Does this solves the problem?



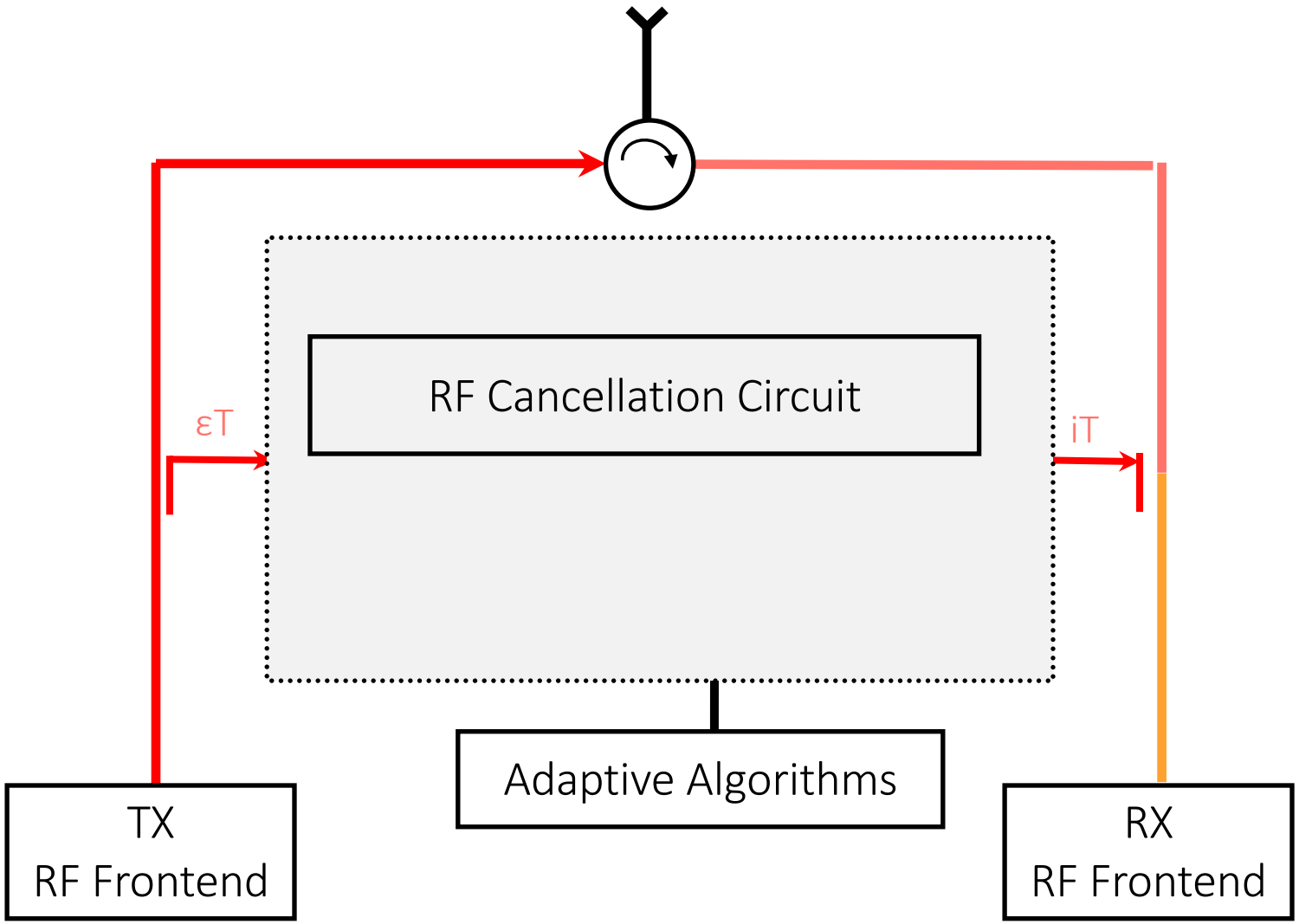
Challenge: Self-Interference is dynamic



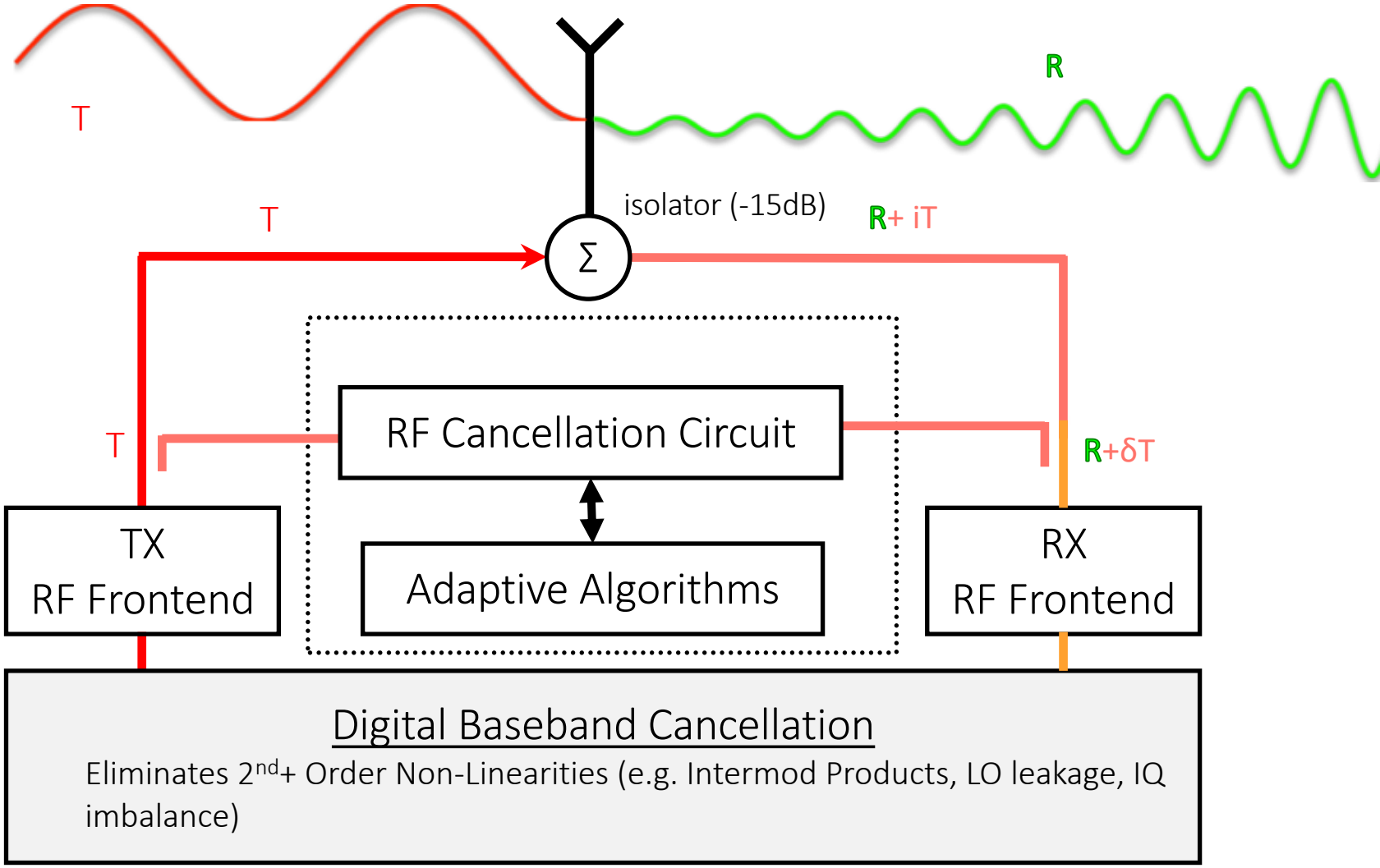
Analog RF Cancellation



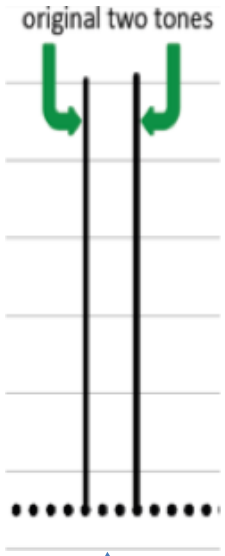
Analog RF Cancellation

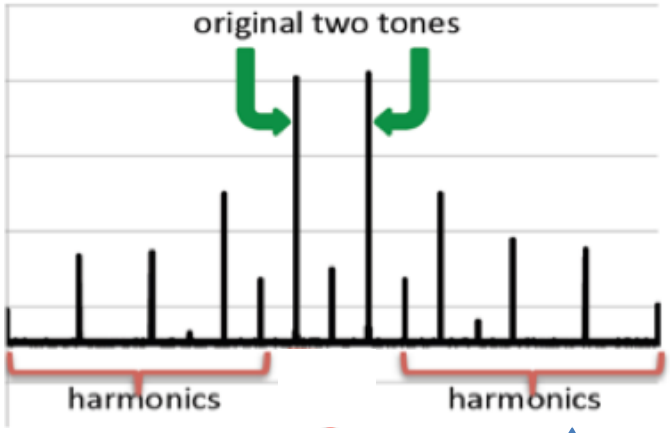


Digital Baseband Cancellation



Digital Baseband Cancellation



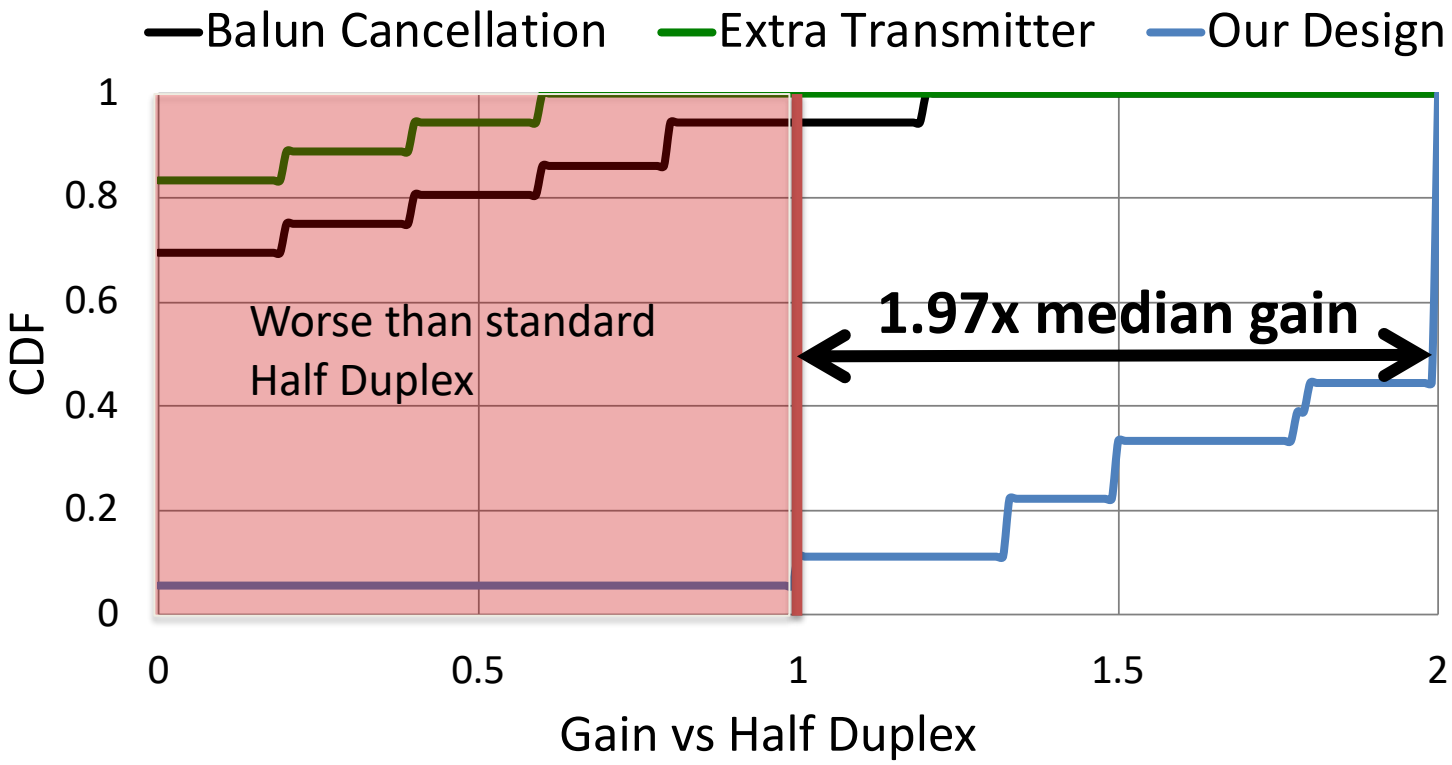


Evaluation: Does that translate to doubling of throughput in practice?

- Testbed: Indoor office noisy environment, various locations for the two full duplex radios.
- Compare throughput achieved in full duplex with that achieved in half duplex
- Full duplex implemented using our approach, and prior balun and extra TX chain based approaches

$$\text{Gain} = \frac{\textbf{Throughput of FD}}{\textbf{Throughput of HD}}$$

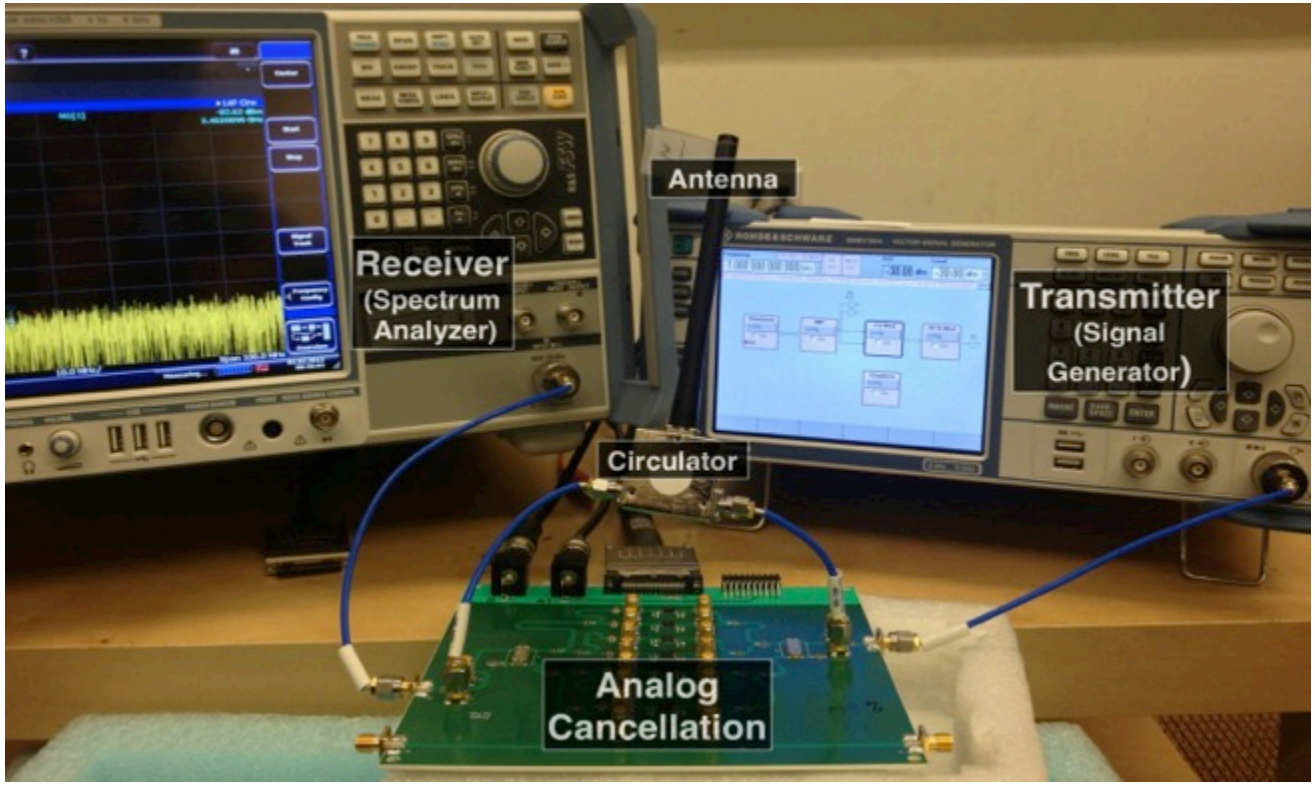
Evaluation Q2: Does that translate to doubling of throughput in practice?



Design achieves the theoretical throughput doubling

Does our design work with the widest WiFi bandwidth of 80MHz?

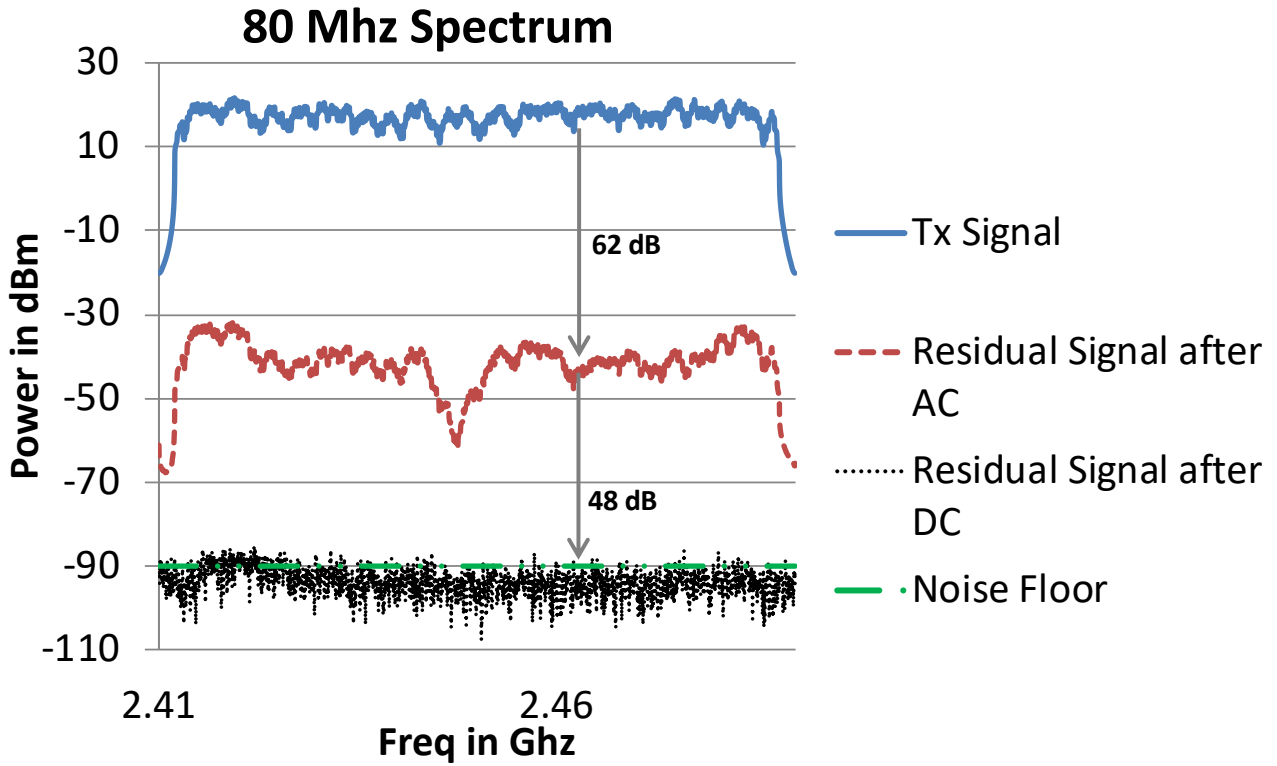
- Implemented using WiFi 802.11ac 80 MHz .
- RS equipment, since other hardware cannot support 80 MHz wideband
- External commercial-grade PA required to boost signal generator's RF output, also introducing non-linearities, obviating any benefit RS equipment afforded us.



Cancellation Performance

80 MHz Bandwidth. WiFi OFDM waveform, 20 dBm TX power at 2.45 GHz

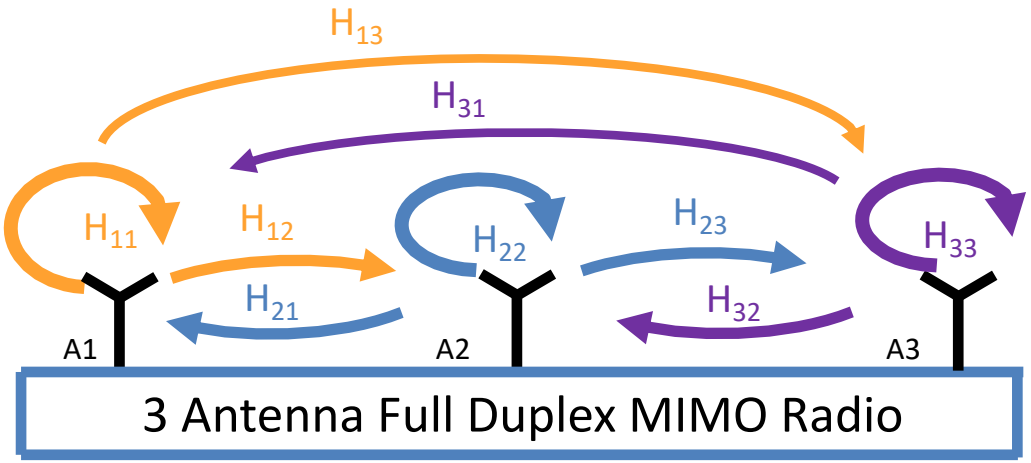
- Wideband
- Tunes to environmental changes within 8us, needs to be re-tuned every 100ms



Analog		Digital		Total
>60dB	+	~50dB	=	>110dB

Full duplex radios: MIMO

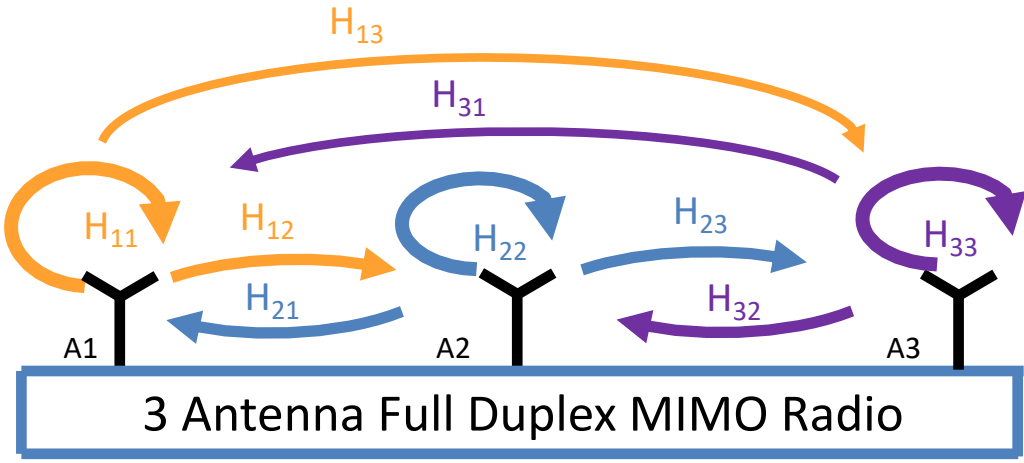
How is the MIMO full duplex problem different?

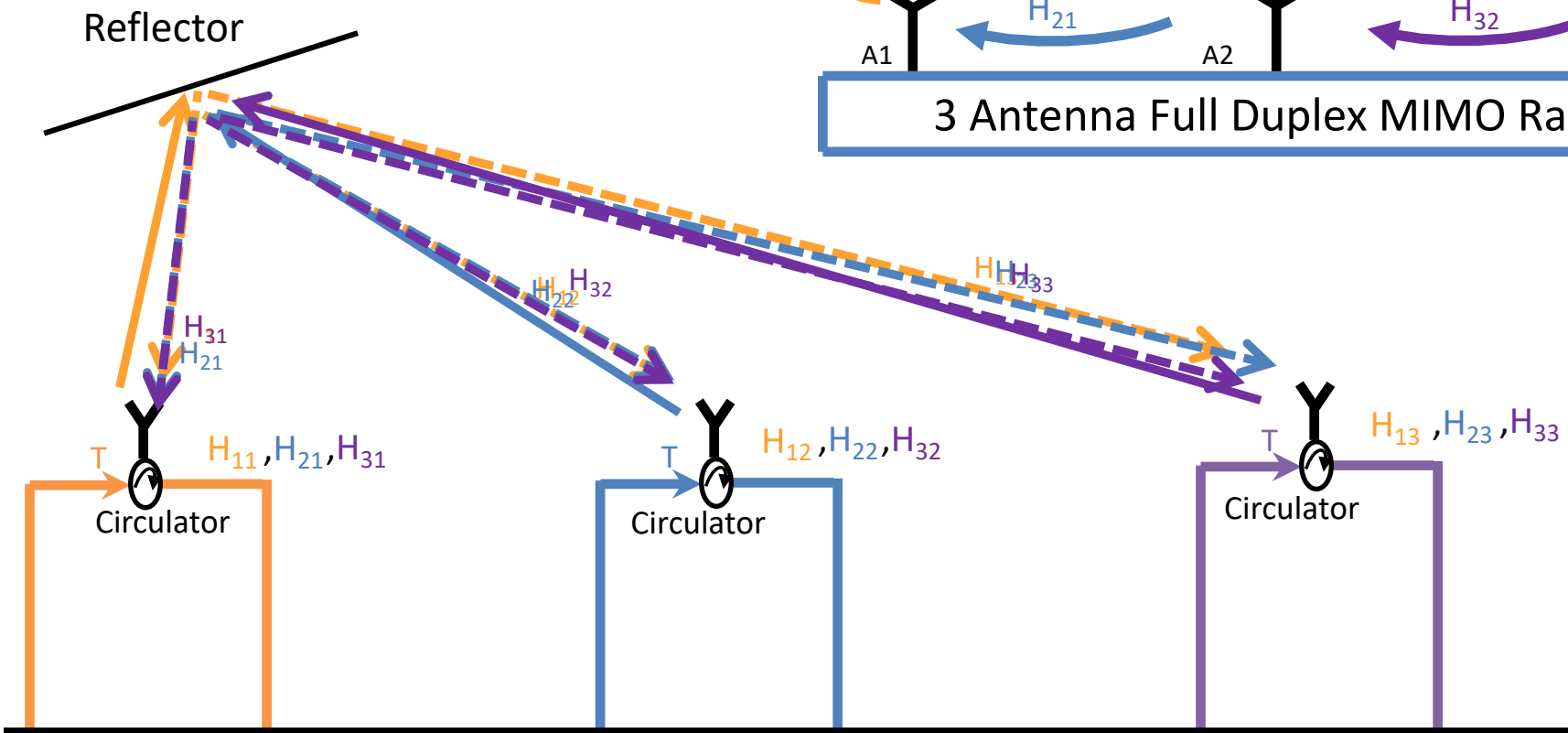


Want:

- Cancellation complexity scales linearly with M (number of antennas).
- Cancellation residue is the same as the SISO full duplex, i.e. it does not degrade with increasing number of antennas.

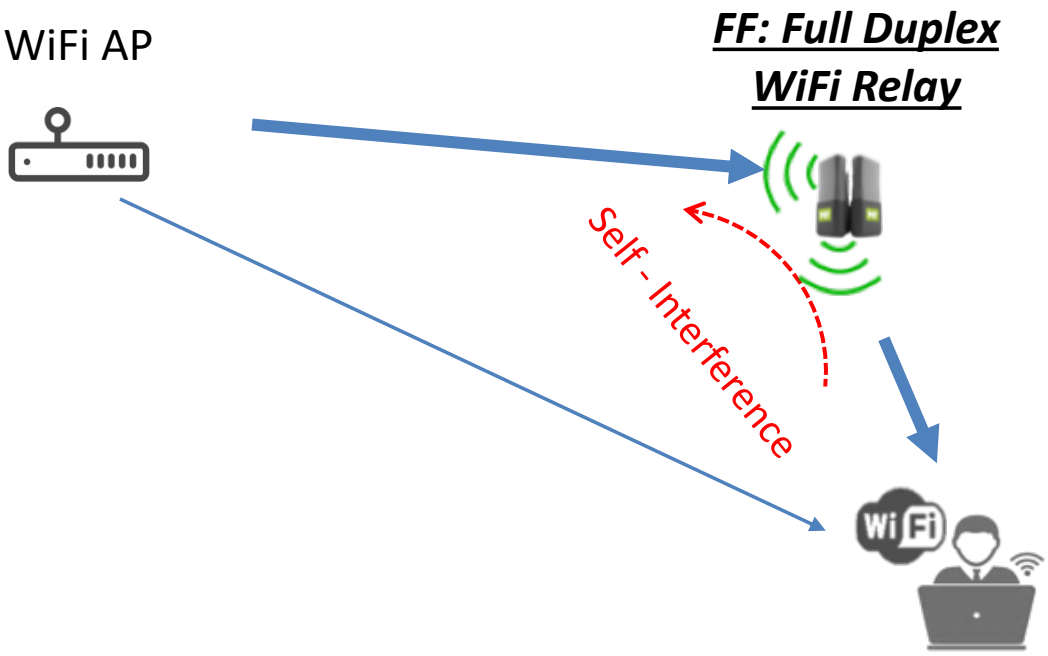
How is the MIMO full duplex problem different?





MIMO full duplex has quadratically more number of signals to cancel because of the presence of cross talk.

FastForward: full duplex relays

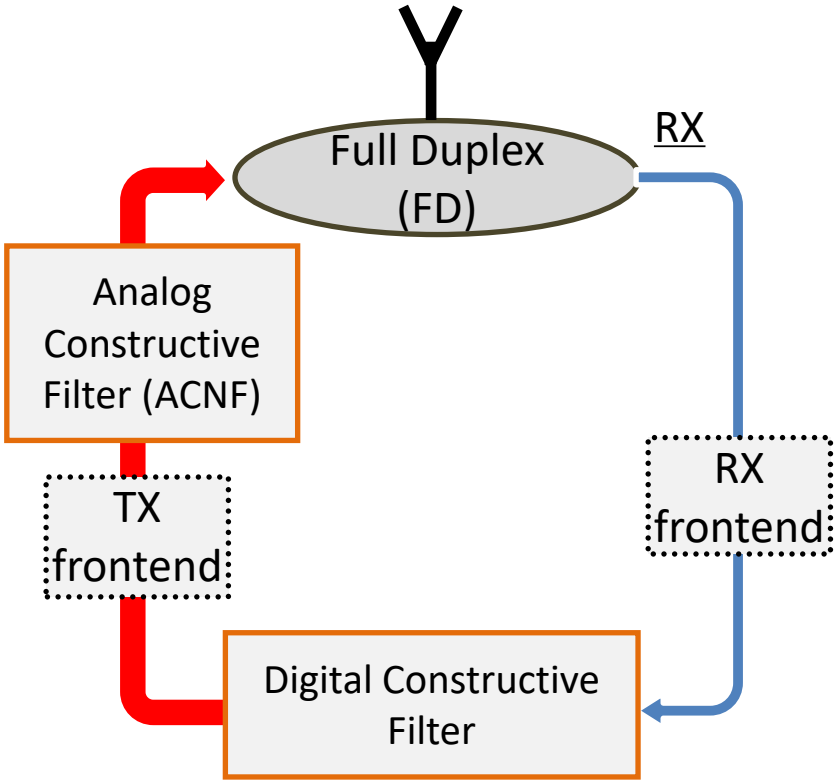


Self-Interference cancellation enables the relay receives a transmission from the AP and re-transmits it after ‘Construct and Forward’ to the client simultaneously

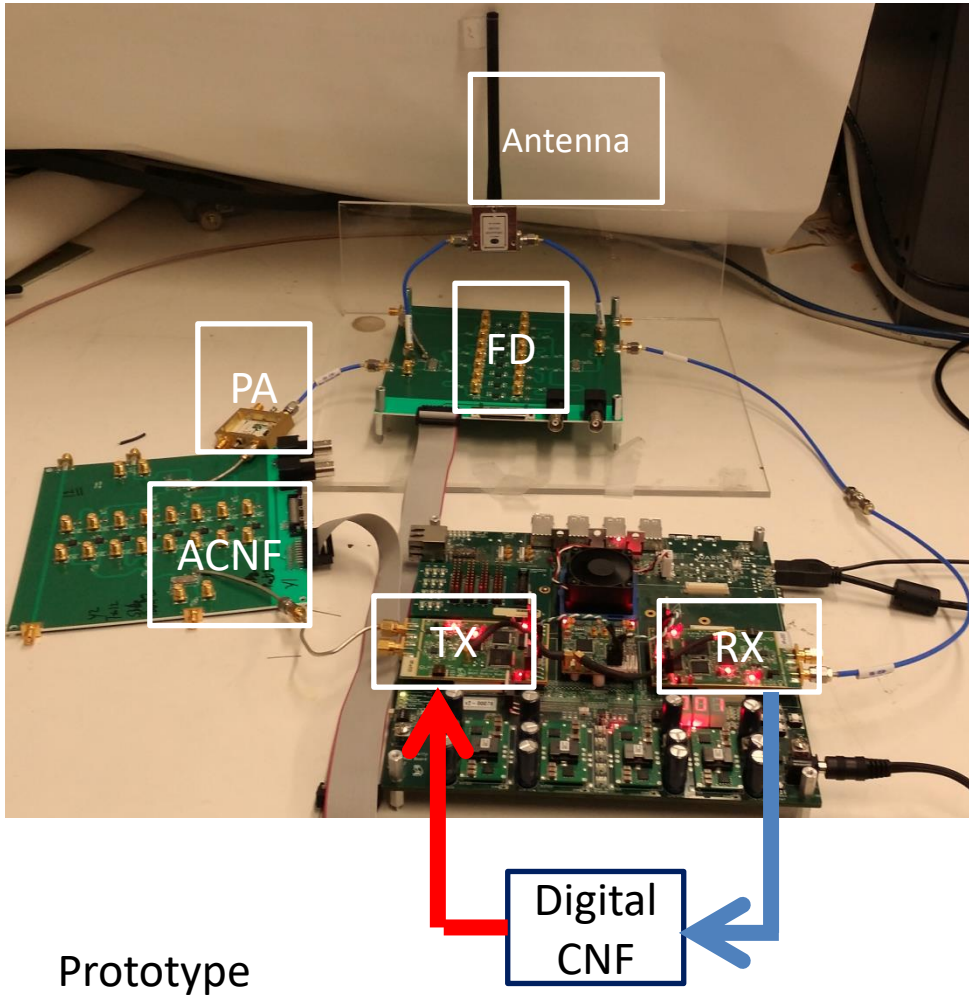
FF designs ‘Construct and Forward’ relaying technique

Implementation of FastForward

- Built using WARP SDR platform, designed for 802.11
- Custom designed construct & forward filter boards & self-interference cancellation
- BW 20MHz, 20dBm TX power
- **Built 2x2 MIMO FF Prototype**



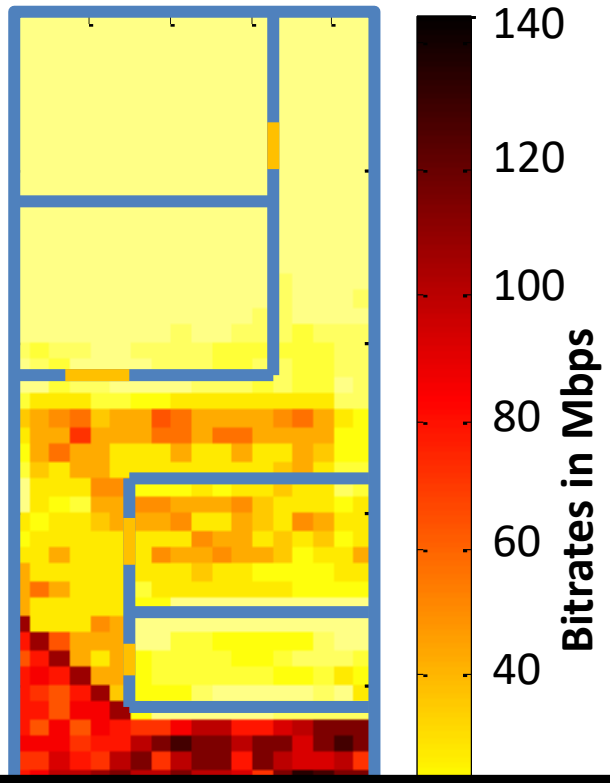
Block Diagram



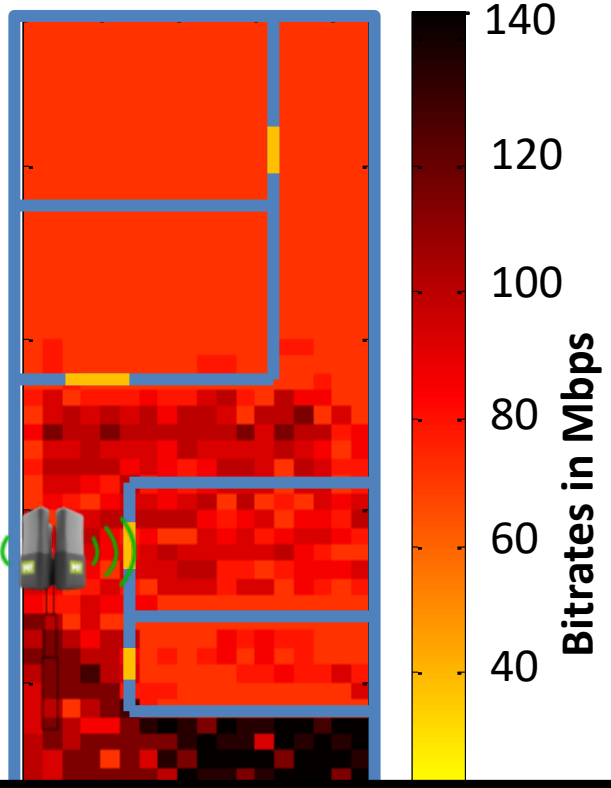
Prototype

FastForward: full duplex relays

Typical WiFi Coverage & Capacity

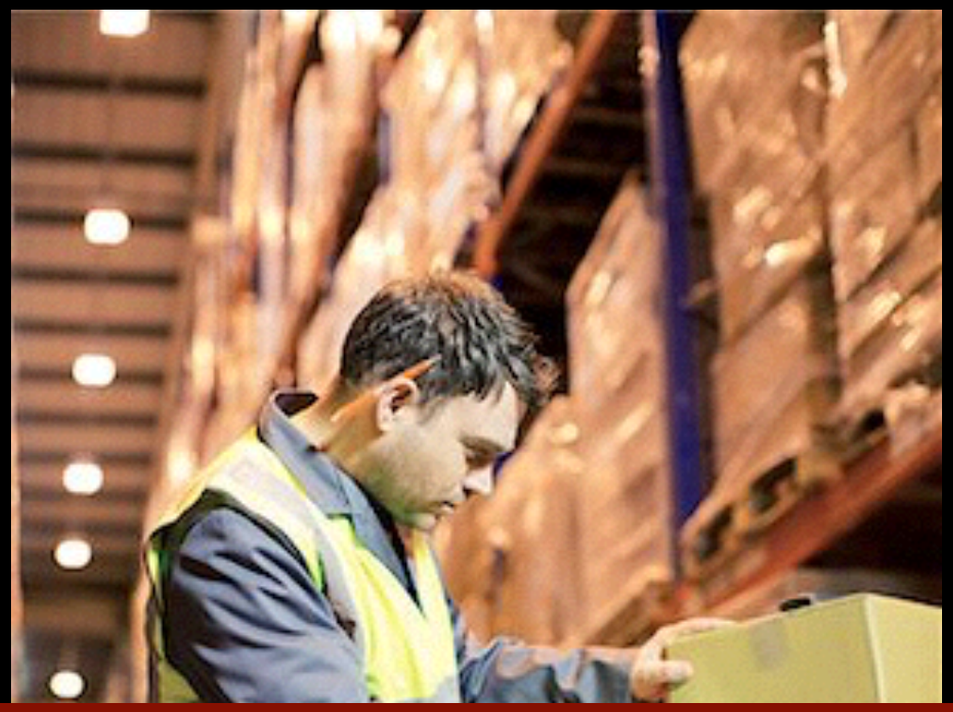


Improved WiFi Coverage & Capacity with full duplex relays



FF works with existing WiFi APs & improves a typical home WiFi network's throughput and range by 2-3x

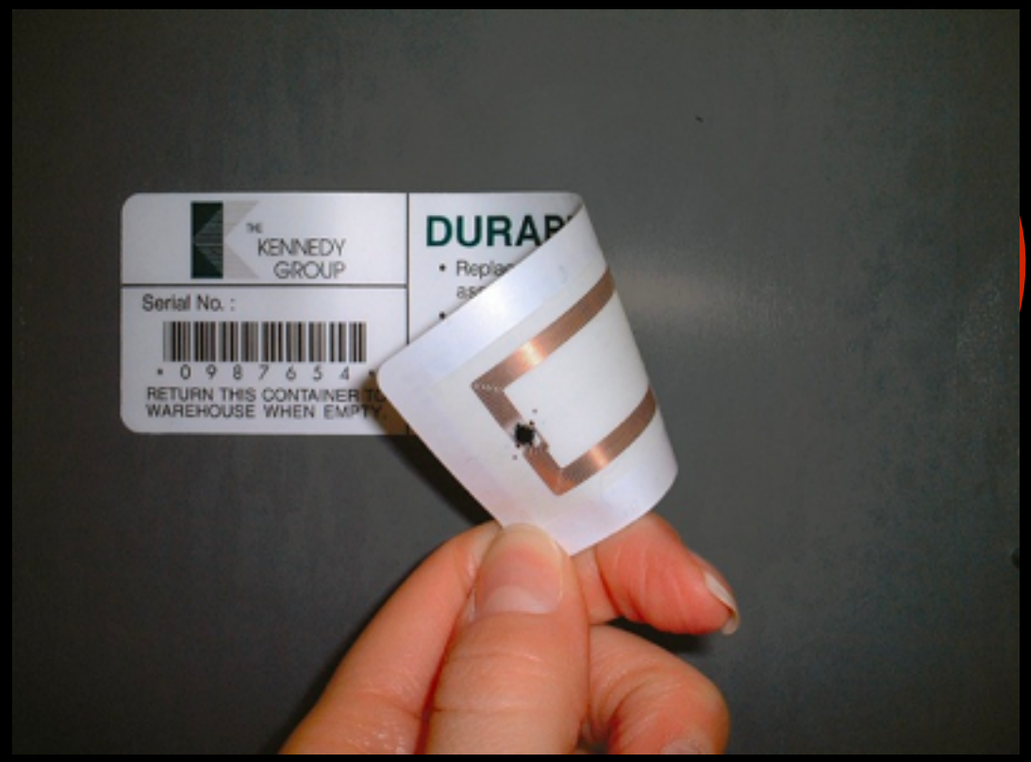
Warehouse Management

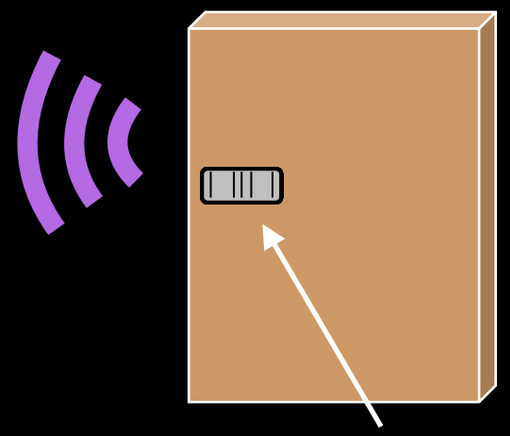


An inventory cycle in a single warehouse takes more than a month (NY Times)

Walmart lost 3 billion dollars in a single year because of inventory mismatch (Fortune)

Battery-Free RFIDs for Inventory Control





5-10 cents each

Read and uniquely identify it from a distance

Battery-free RFIDs are fundamentally crippled by their limited communication range

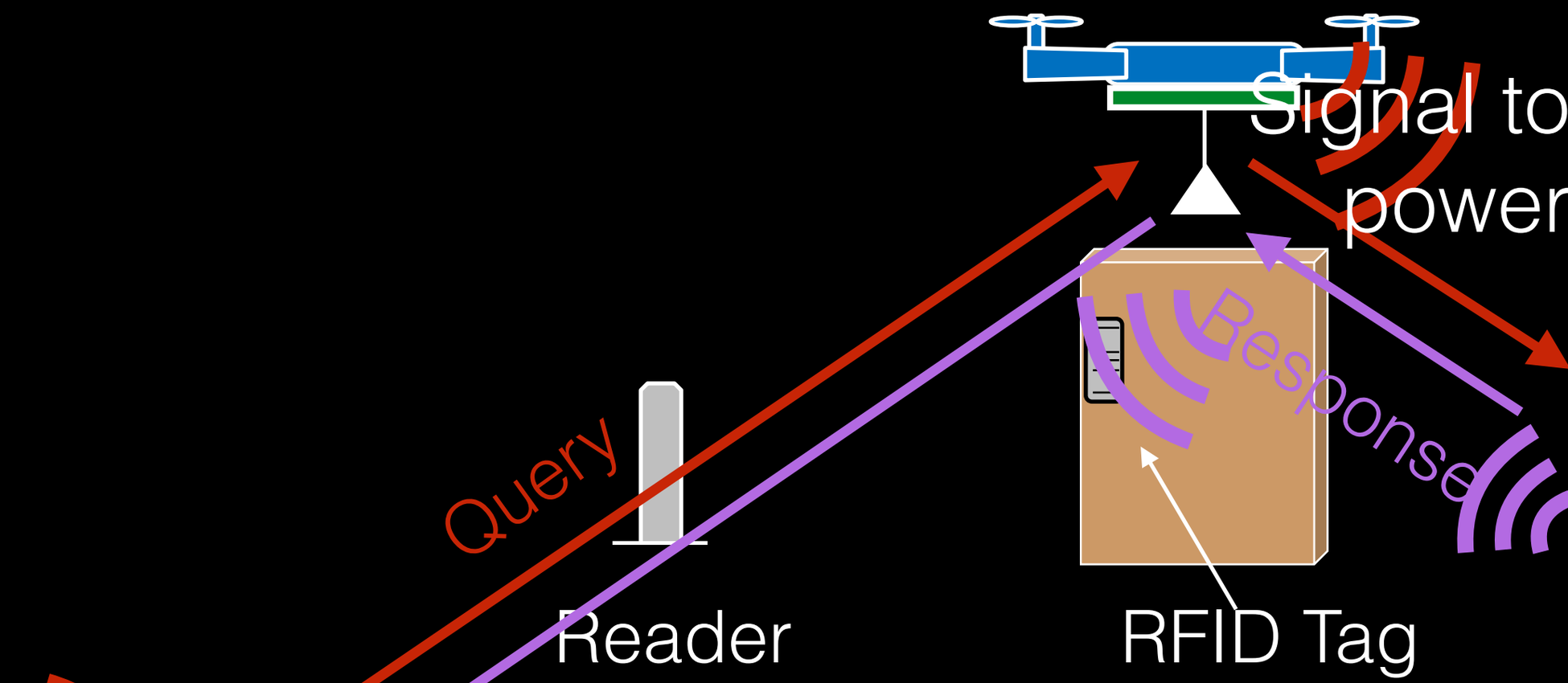
Reader

Reader

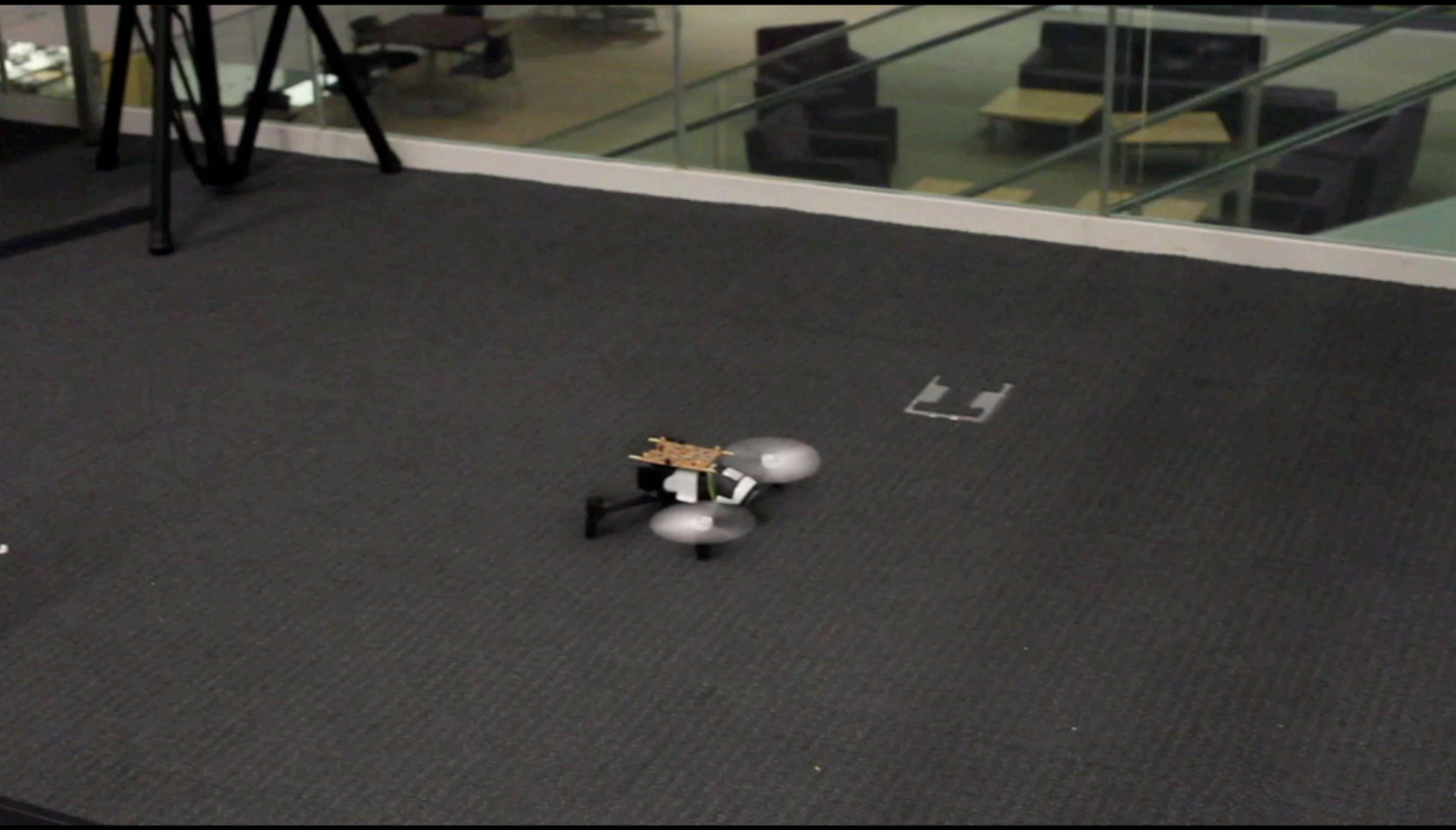
tens of centimeters to few meters

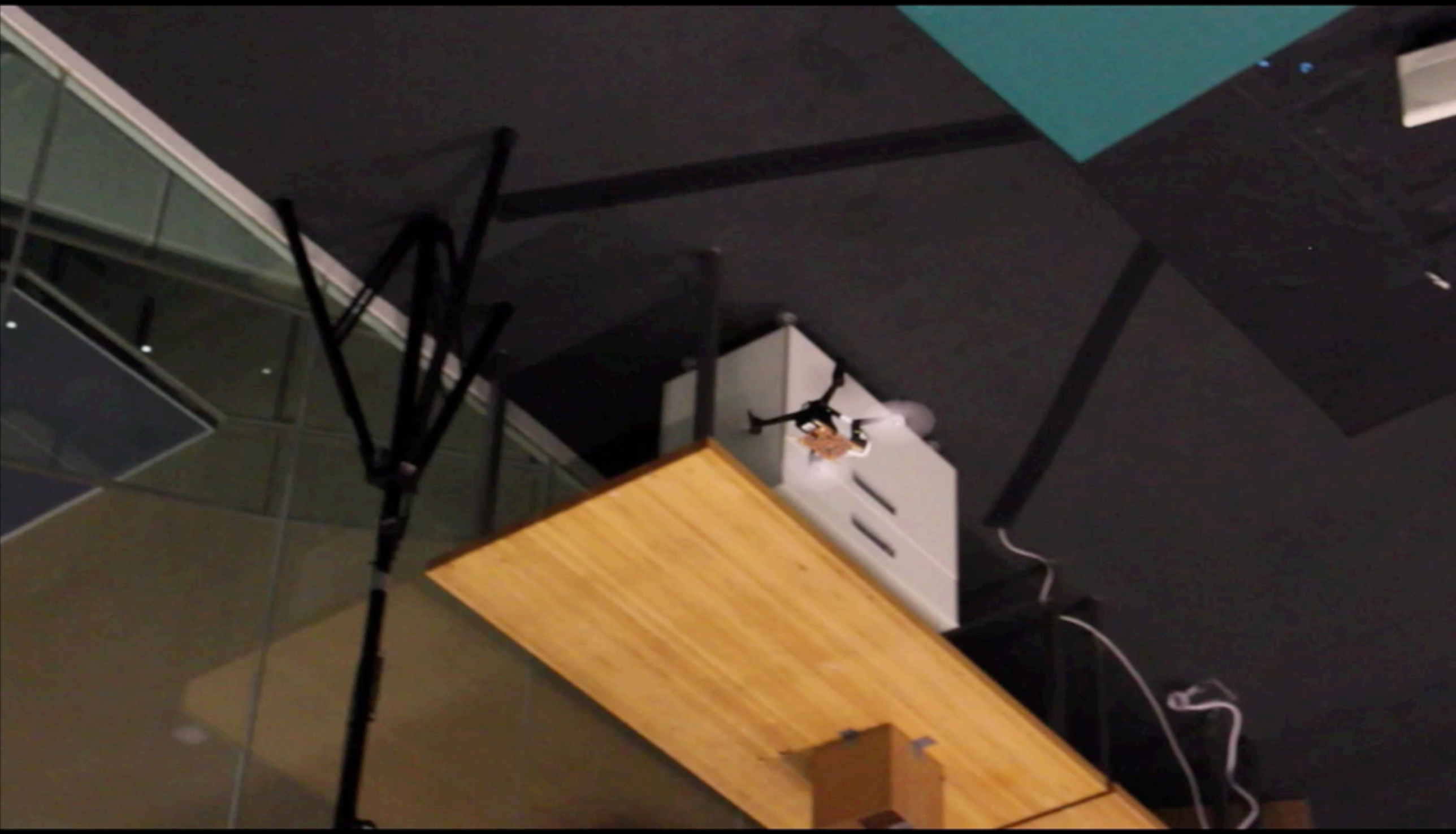
RFly: Enabling wide-area battery-free sensing and localization using drone relays

RFly: Enabling wide-area battery-free sensing and localization using drone relays



- Eliminates blind spots
- Accurately localizes
- Transparent to existing RFID infrastructure

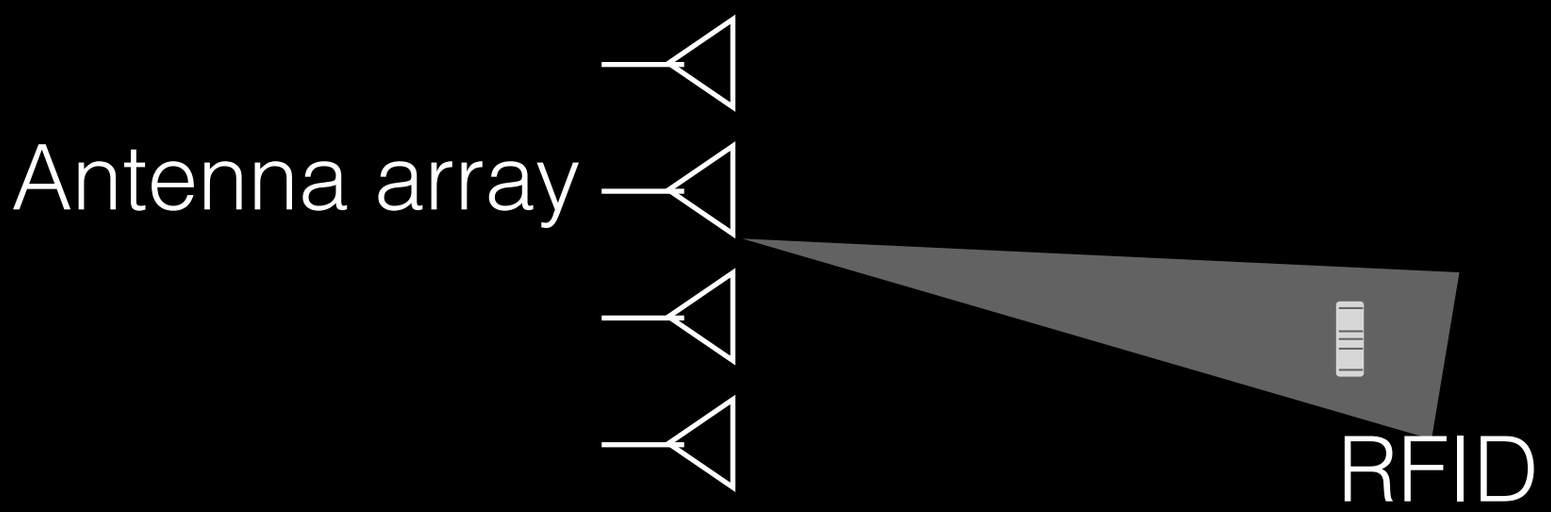




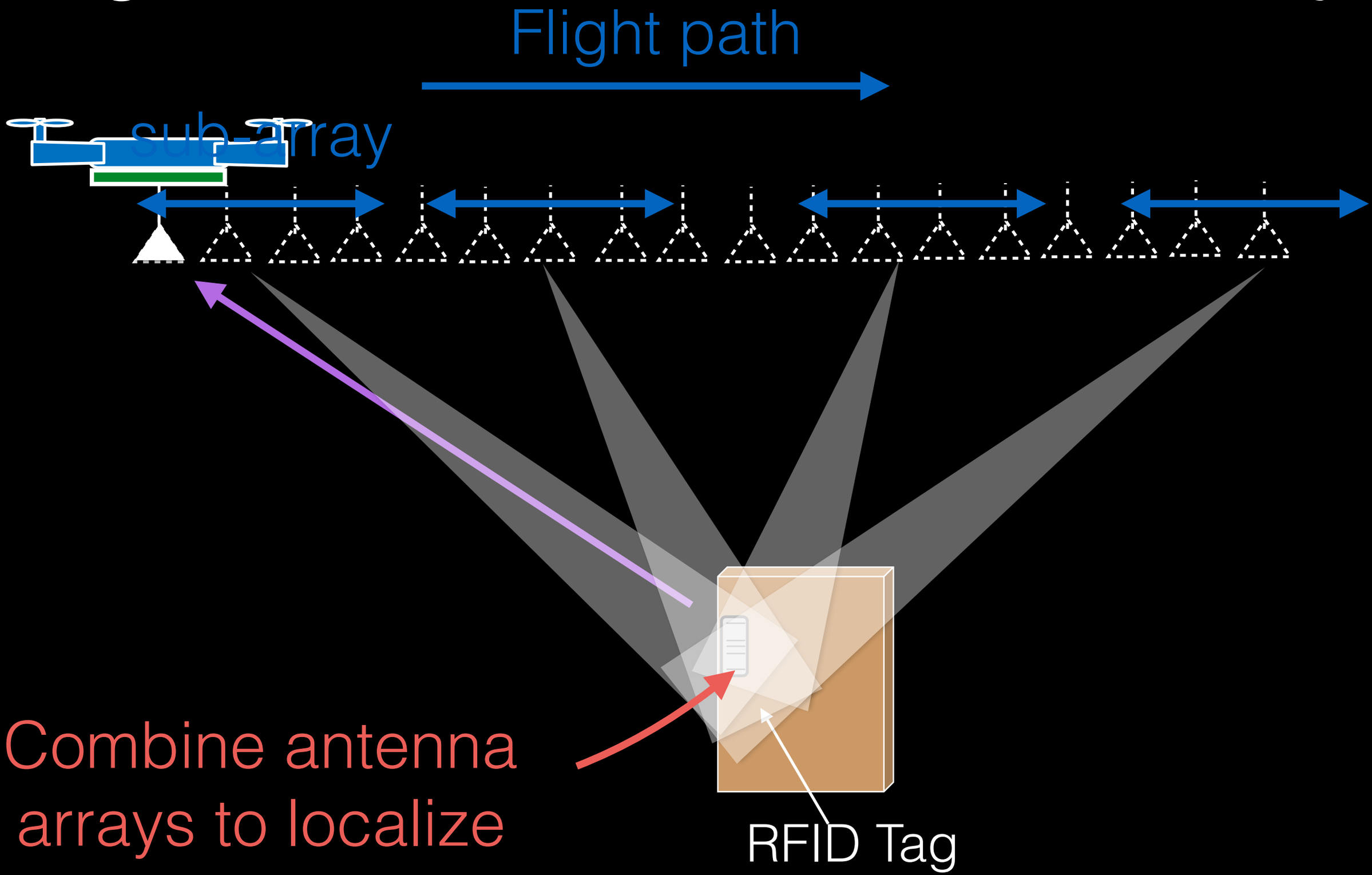
How can we localize through a mobile relay?

How can we localize through a mobile relay?

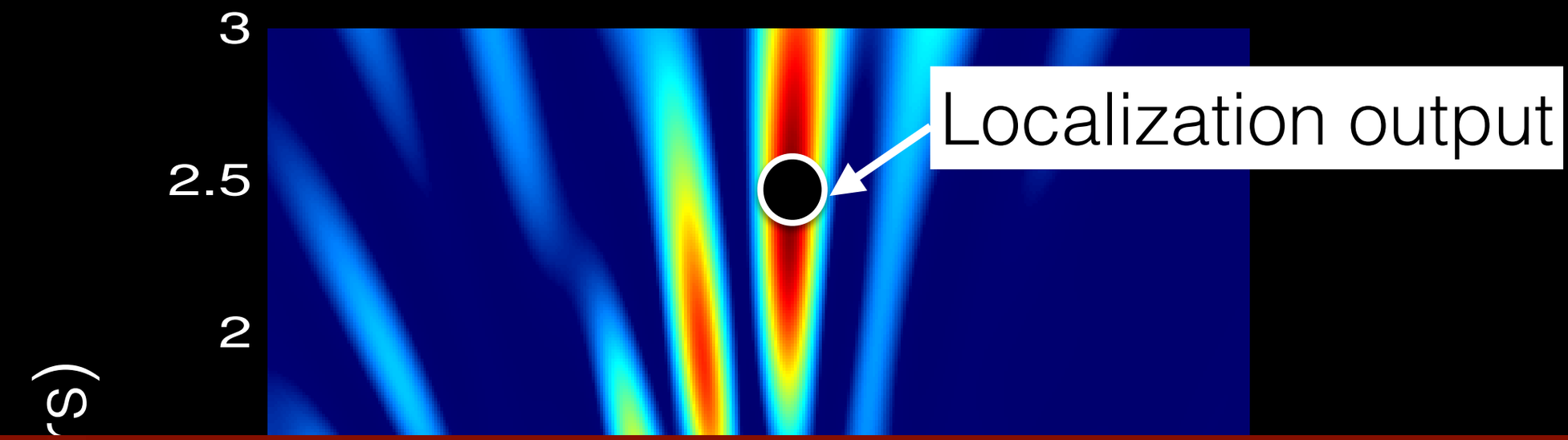
- State-of-the-art localization proposals leverage antenna arrays
  - ArrayTrack [NSDI'13], PinPoint [NSDI'13], PinIt [SIGCOMM'13], RFIDraw [SIGCOMM'14], UbiCarse [MobiCom'14]



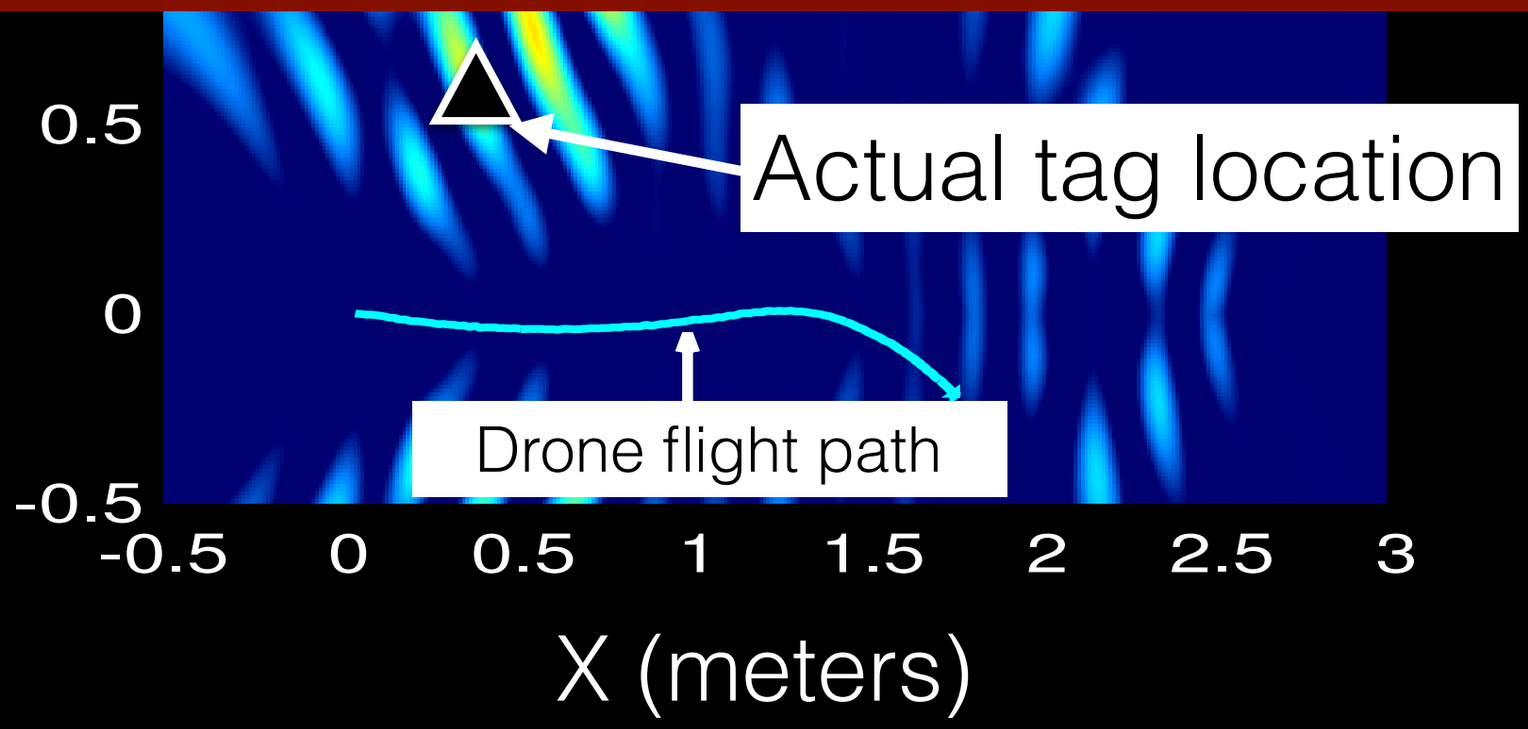
Flight Path Emulates Antenna Array



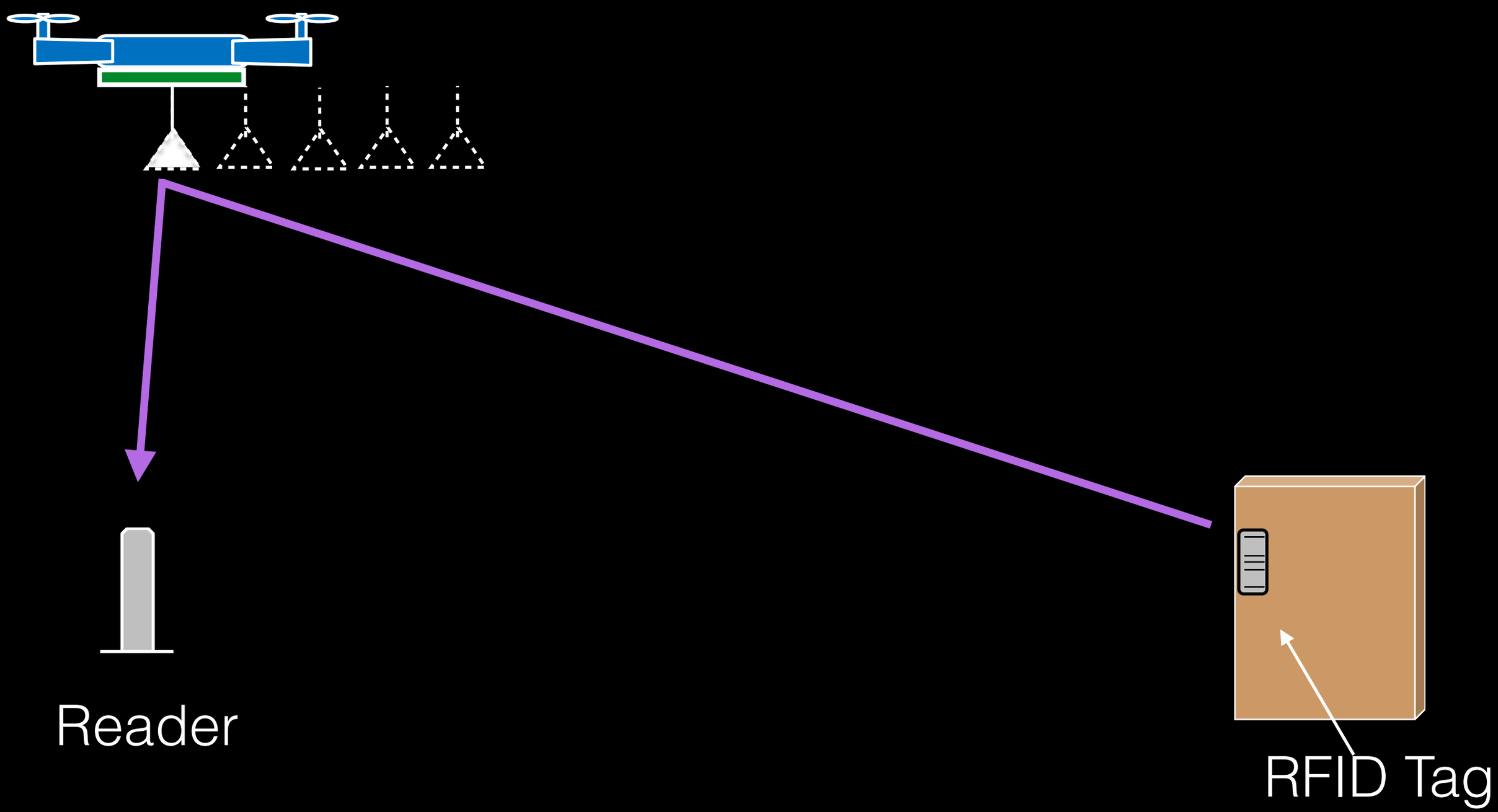
Antenna array-based localization



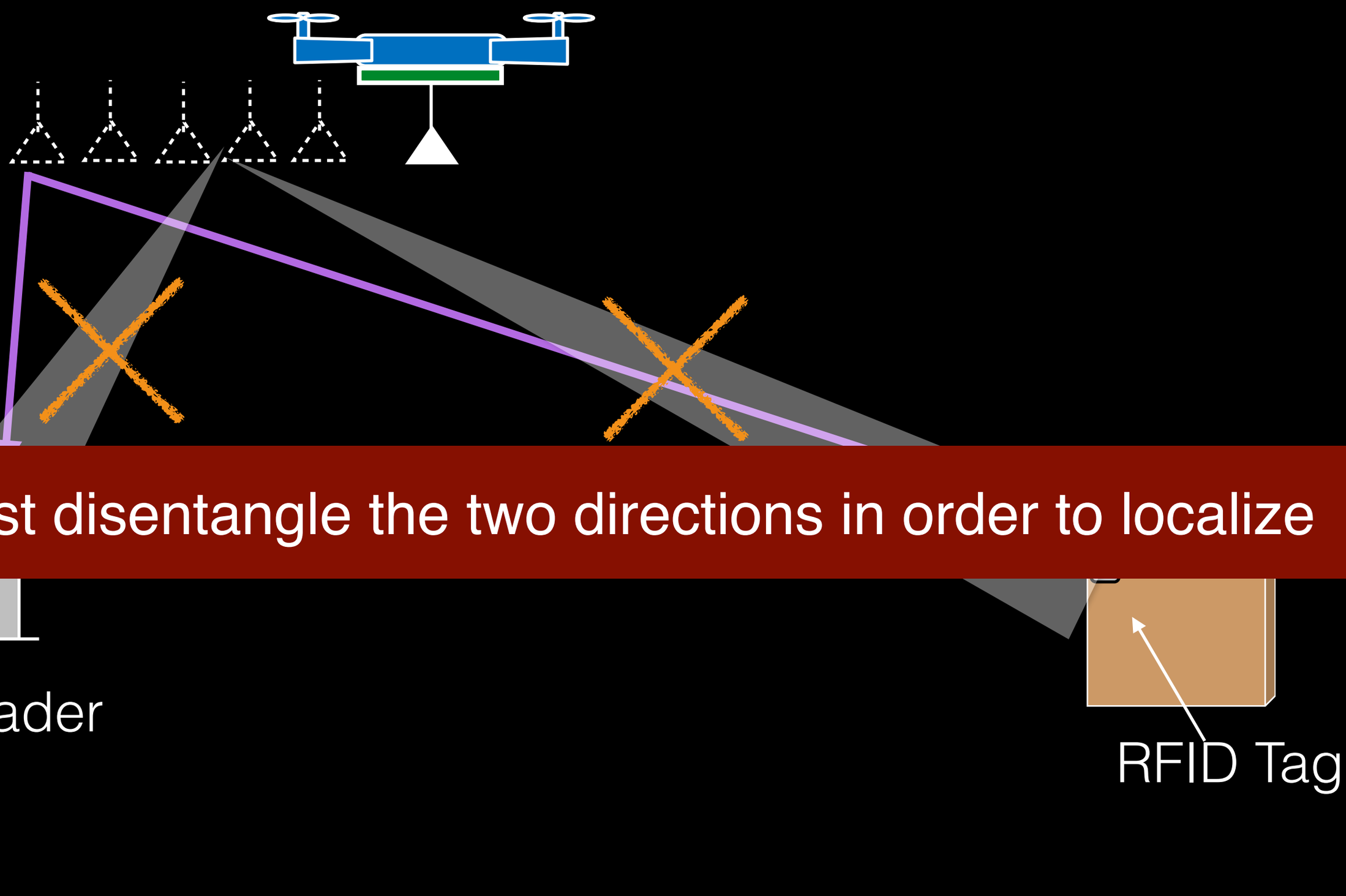
Standard antenna array model fails for through-relay localization



<u>Problem:</u> The reader obtains a re-directed link not a direct link



Problem: The reader obtains a re-directed link not a direct link



Solution Idea: Employ a backscatter mechanism in the relay

Antenna array localization hinges on phase measurements

distance

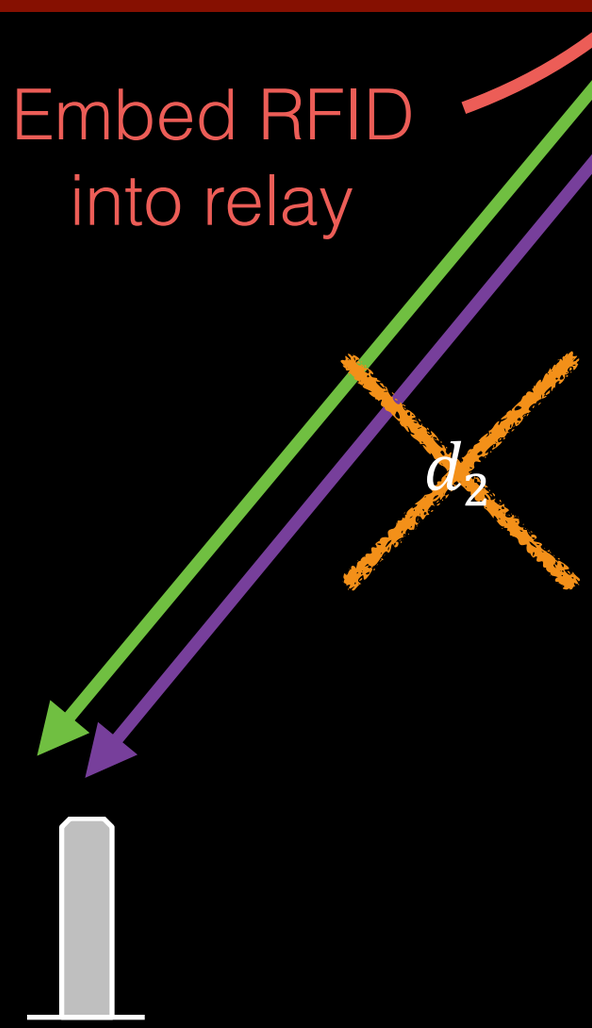
$$\text{Phase } \phi = 2\pi \frac{d}{\lambda}$$

wavelength

Solution Idea: Employ a backscatter mechanism in the relay

Disentangle the two directions and apply antenna array equations on each of them independently

Embed RFID into relay

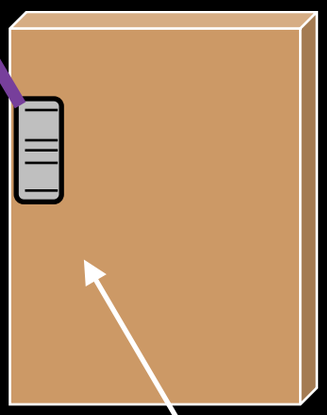


iterate

$$\phi_{RFID} = 2\pi \frac{d_1 + d_2}{\lambda}$$

$$\phi_{relay} = 2\pi \frac{d_2}{\lambda}$$

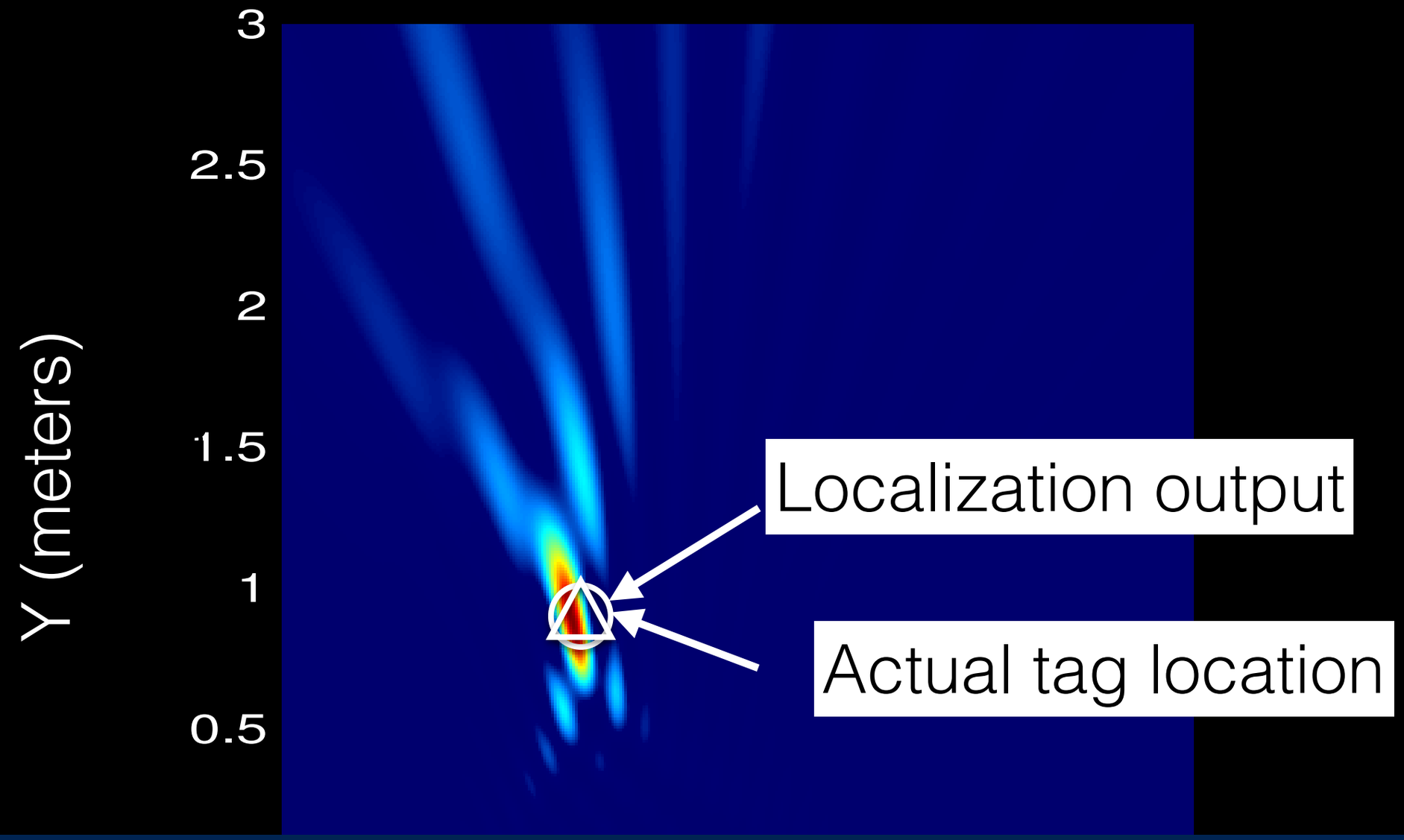
$$\phi_{RFID} - \phi_{relay} = 2\pi \frac{d_1}{\lambda}$$



RFID Tag

Reader

RFly's Localization Algorithm



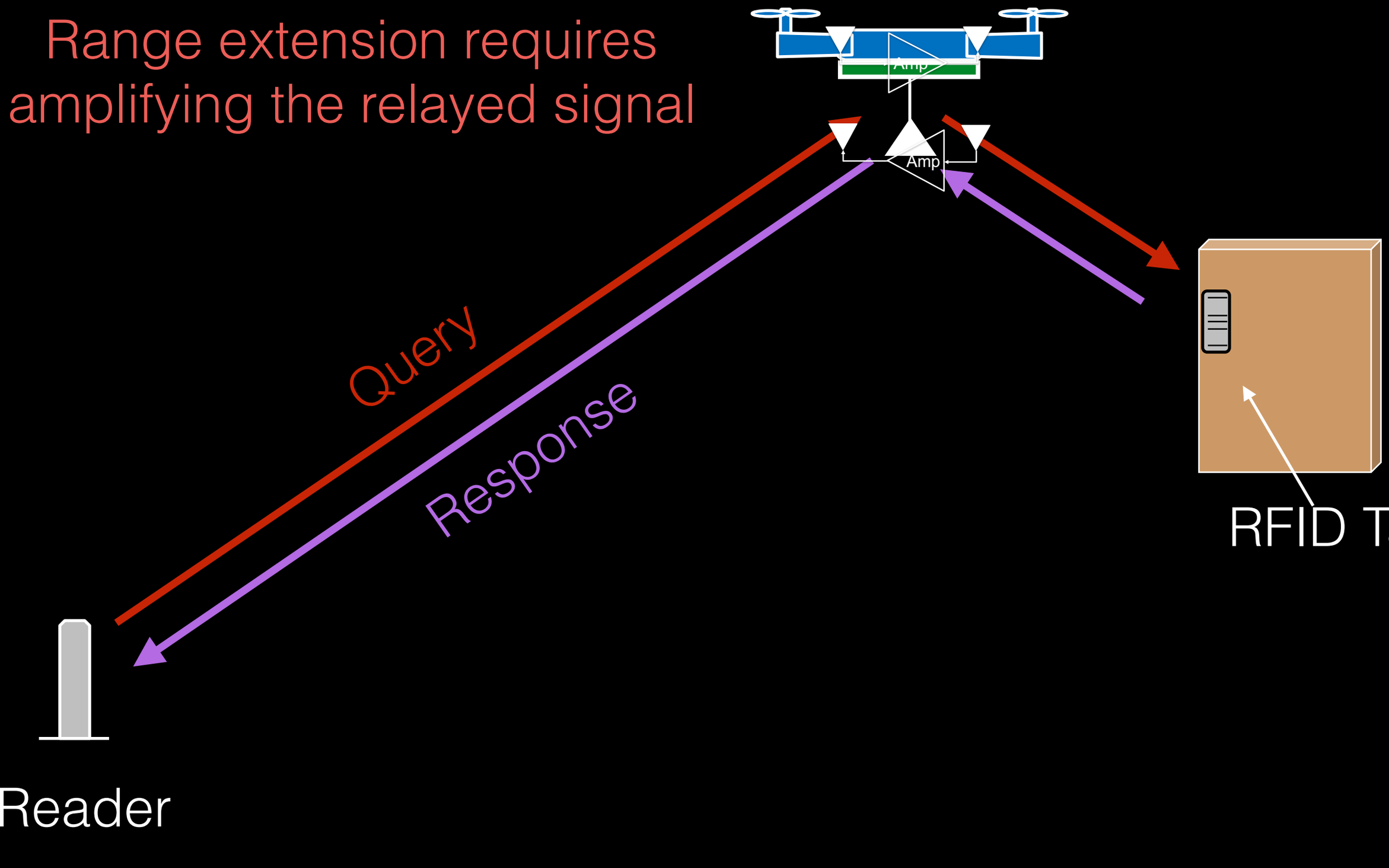
Extend RFly's localization algorithm to address dense multi-path in indoor environments

X (meters)

How can we preserve the phase through a relay while extending the range?

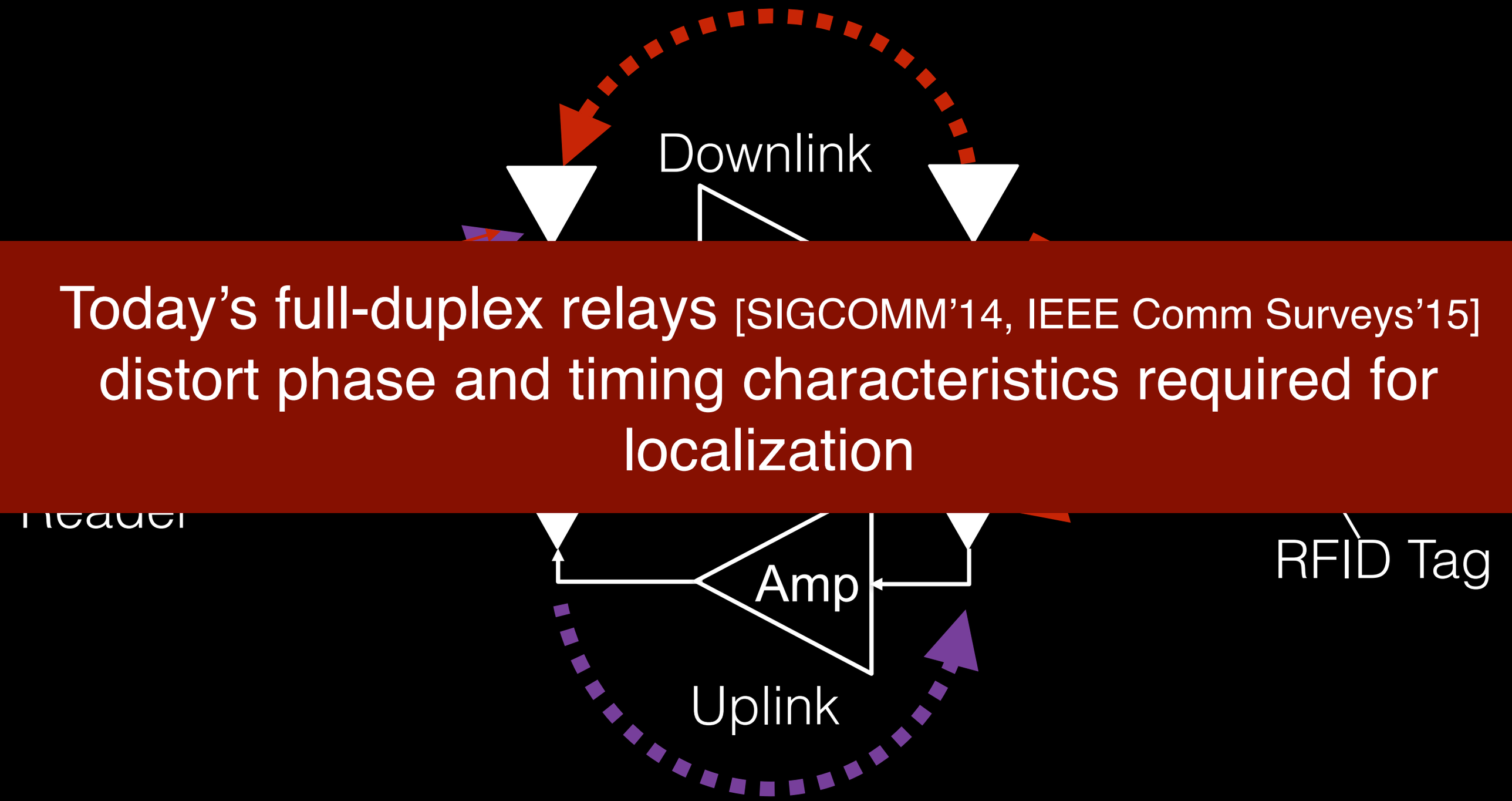
How can we preserve the phase through a relay while extending the range?

Range extension requires amplifying the relayed signal



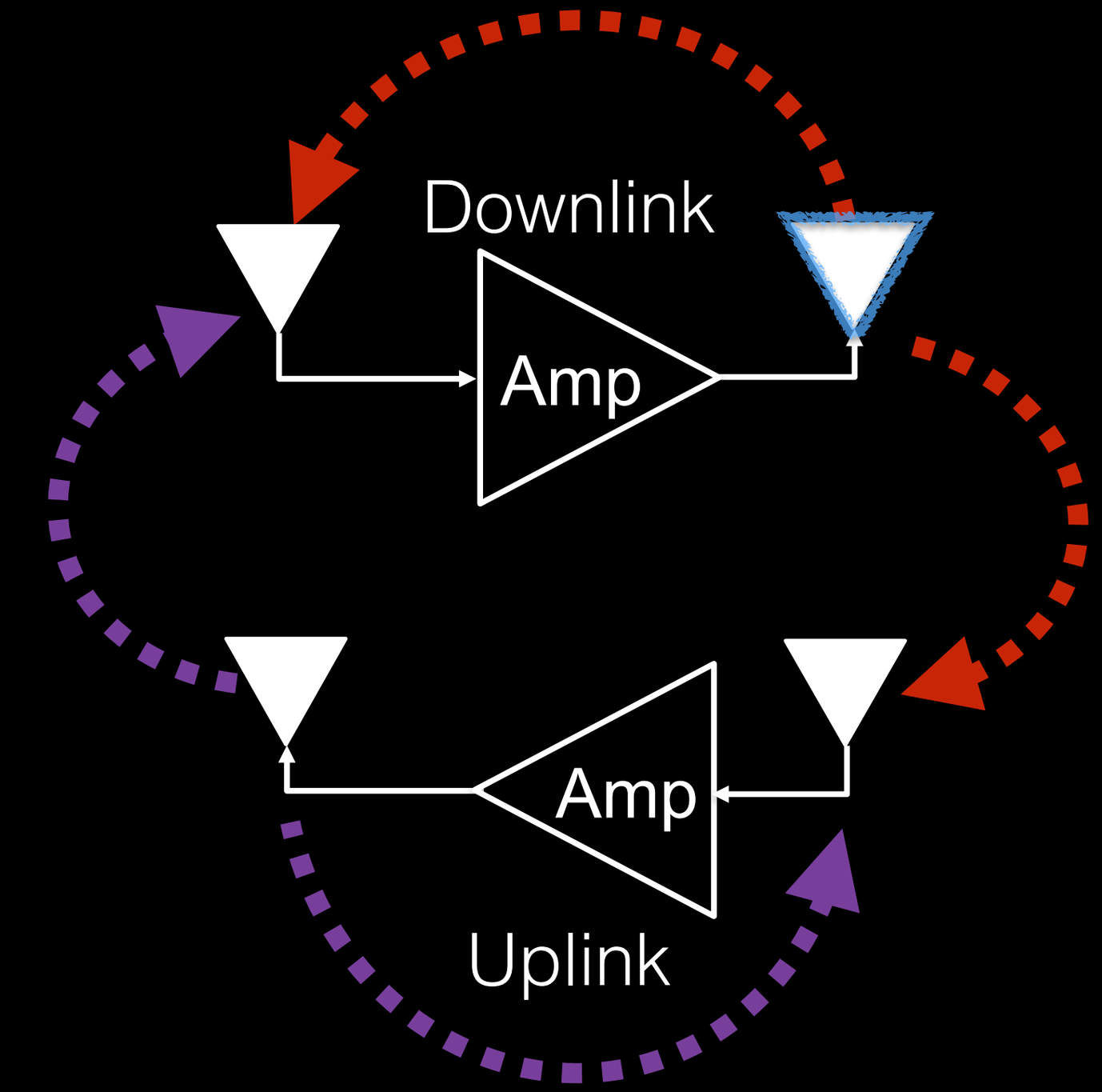
Problem: More amplification results in more self-interference

Four sources of self-interference

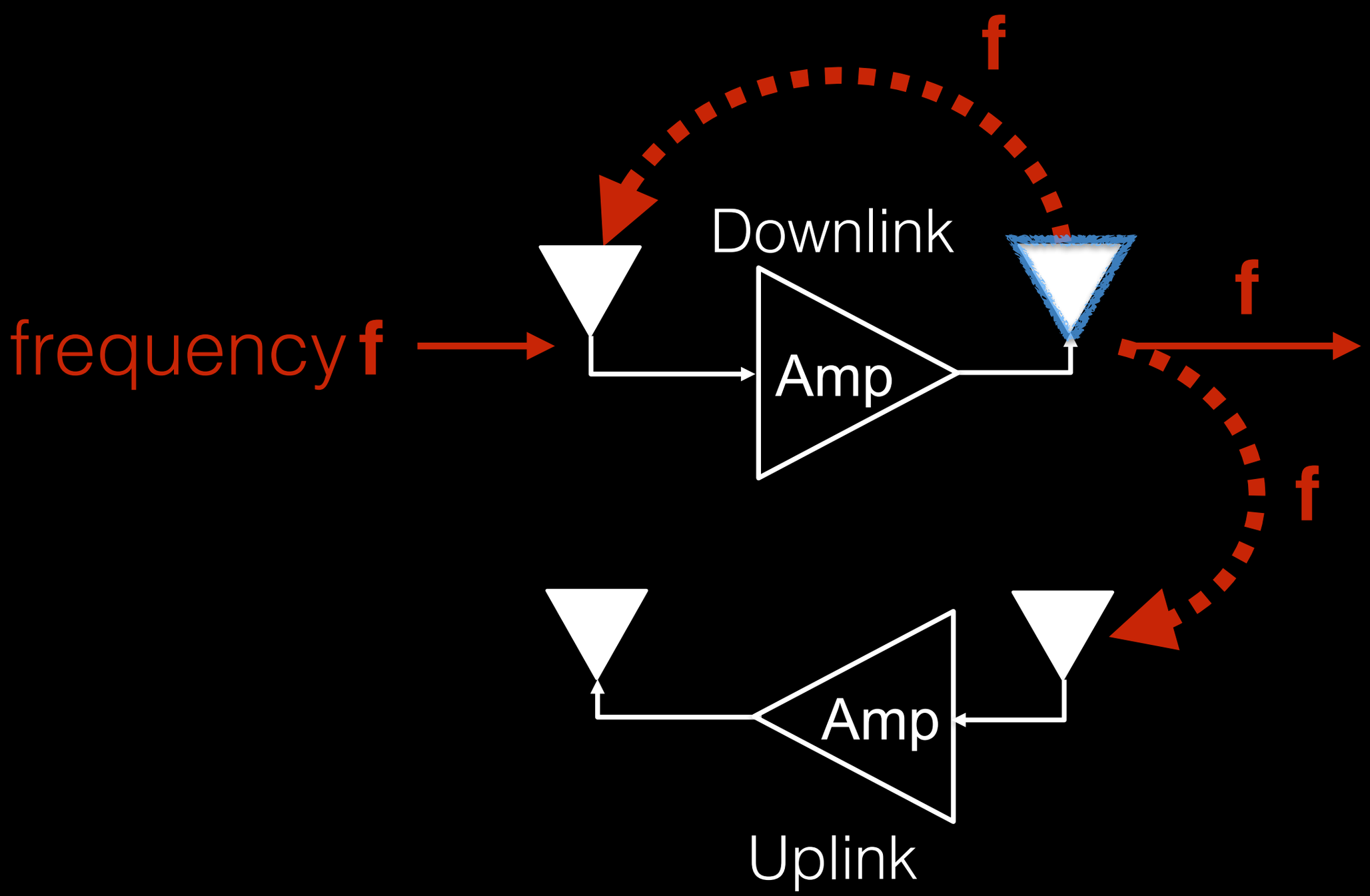


Today's full-duplex relays [SIGCOMM'14, IEEE Comm Surveys'15] distort phase and timing characteristics required for localization

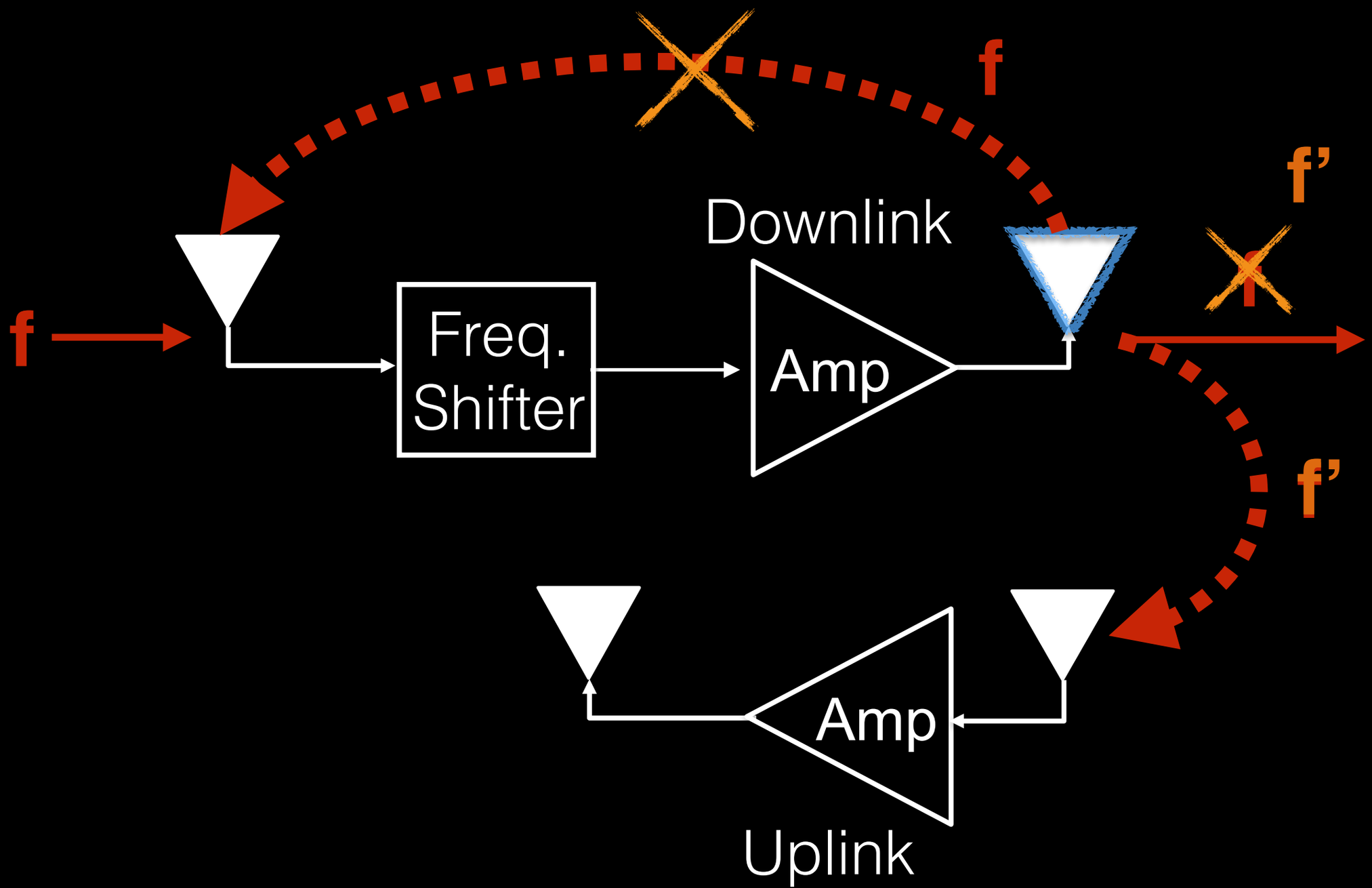
RFly cancels self-interference entirely in the analog domain



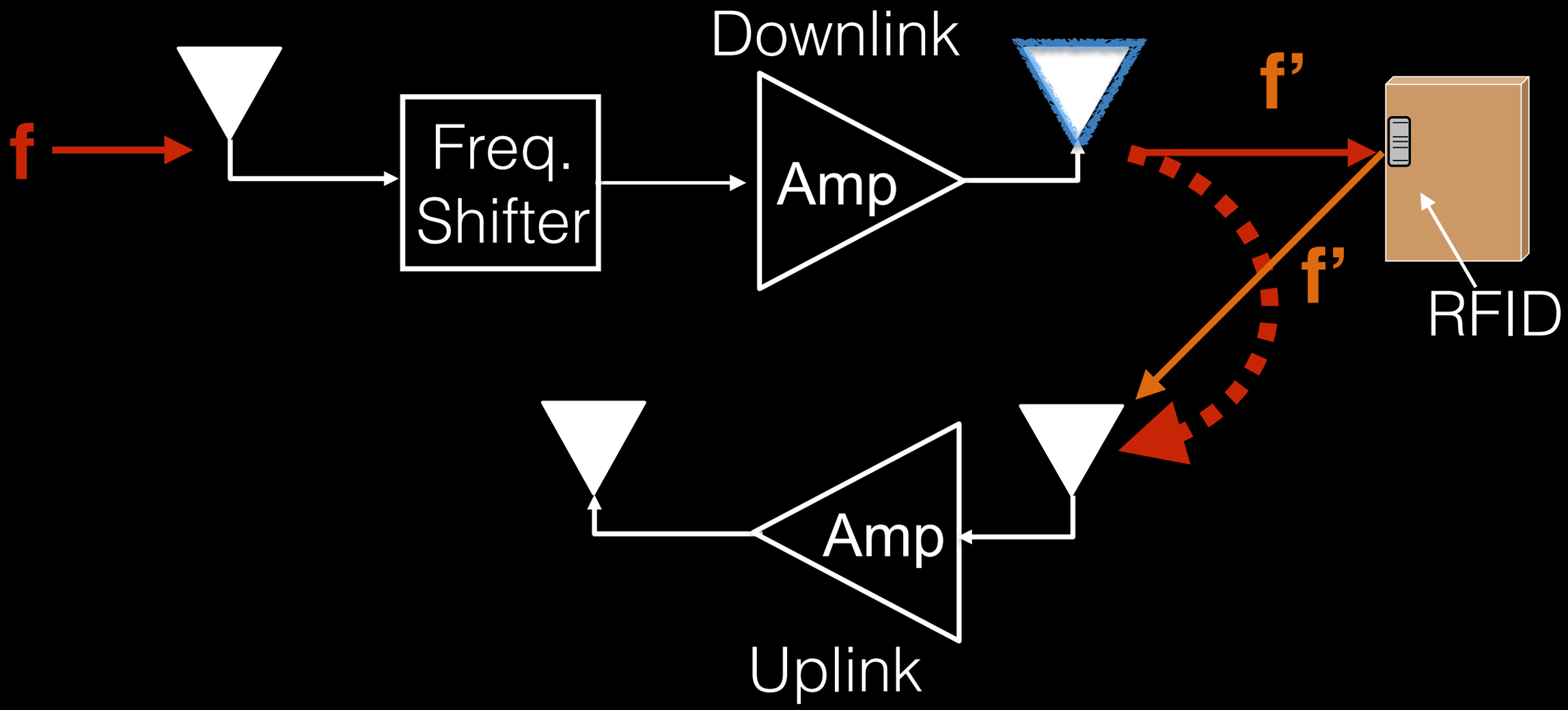
RFly cancels self-interference entirely in the analog domain



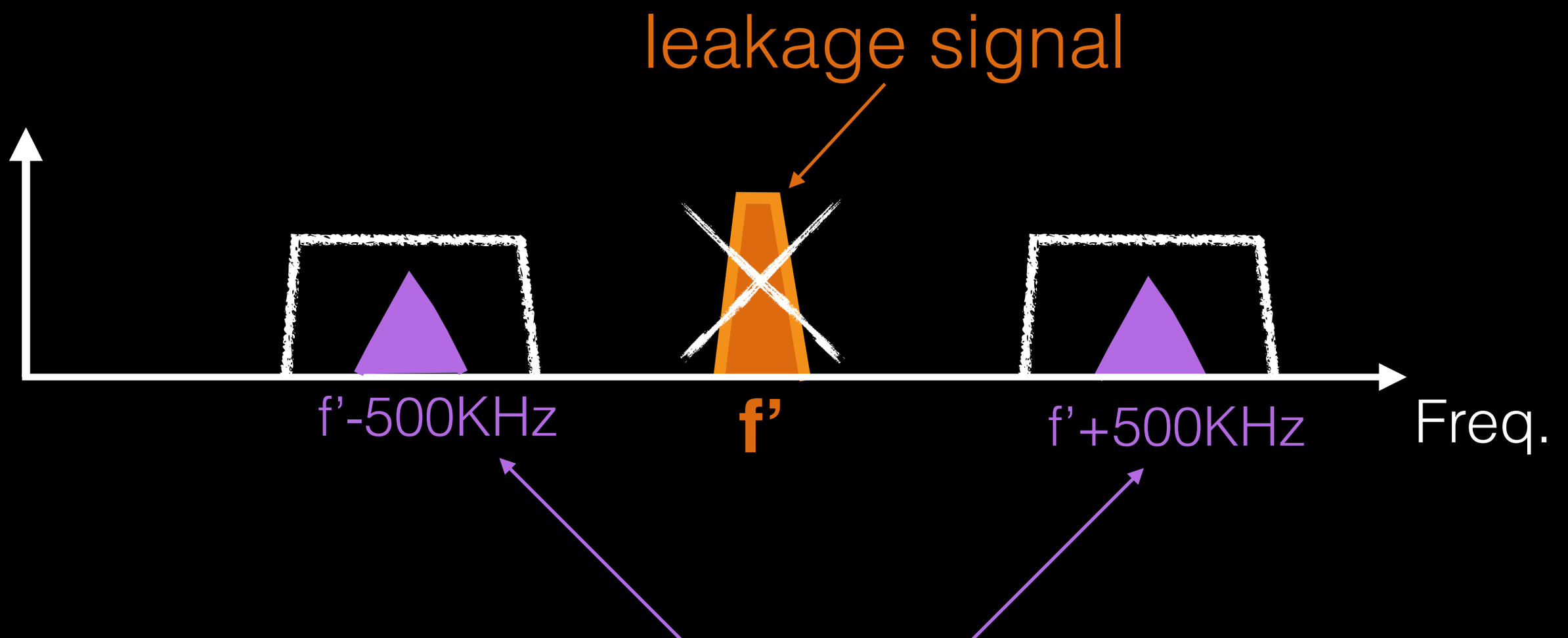
RFly incorporates a frequency shifting mechanism to eliminate interference between output and input



Problem: RFIDs operate by reflecting received signal

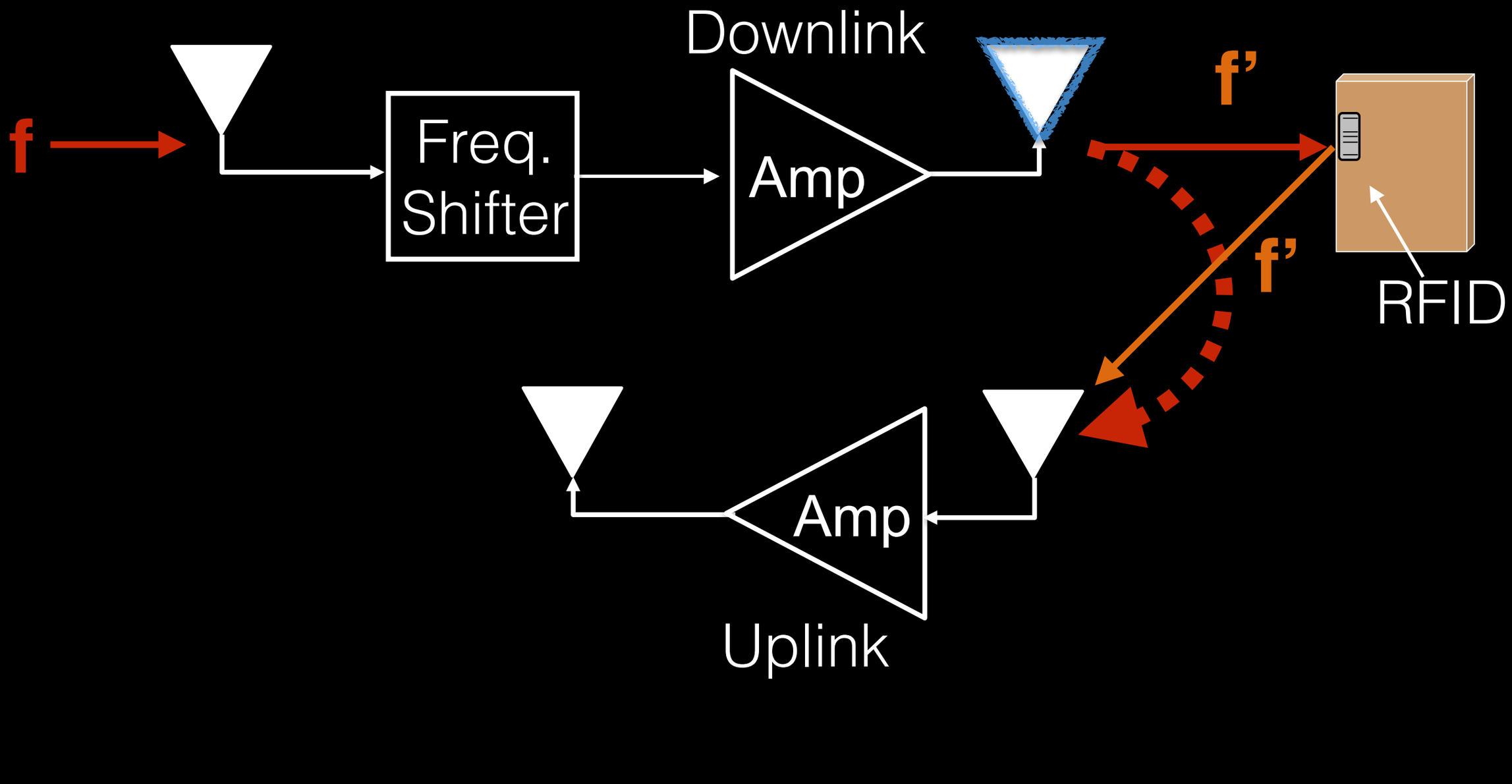


Solution Idea: Exploit the signal structure of backscatter communication

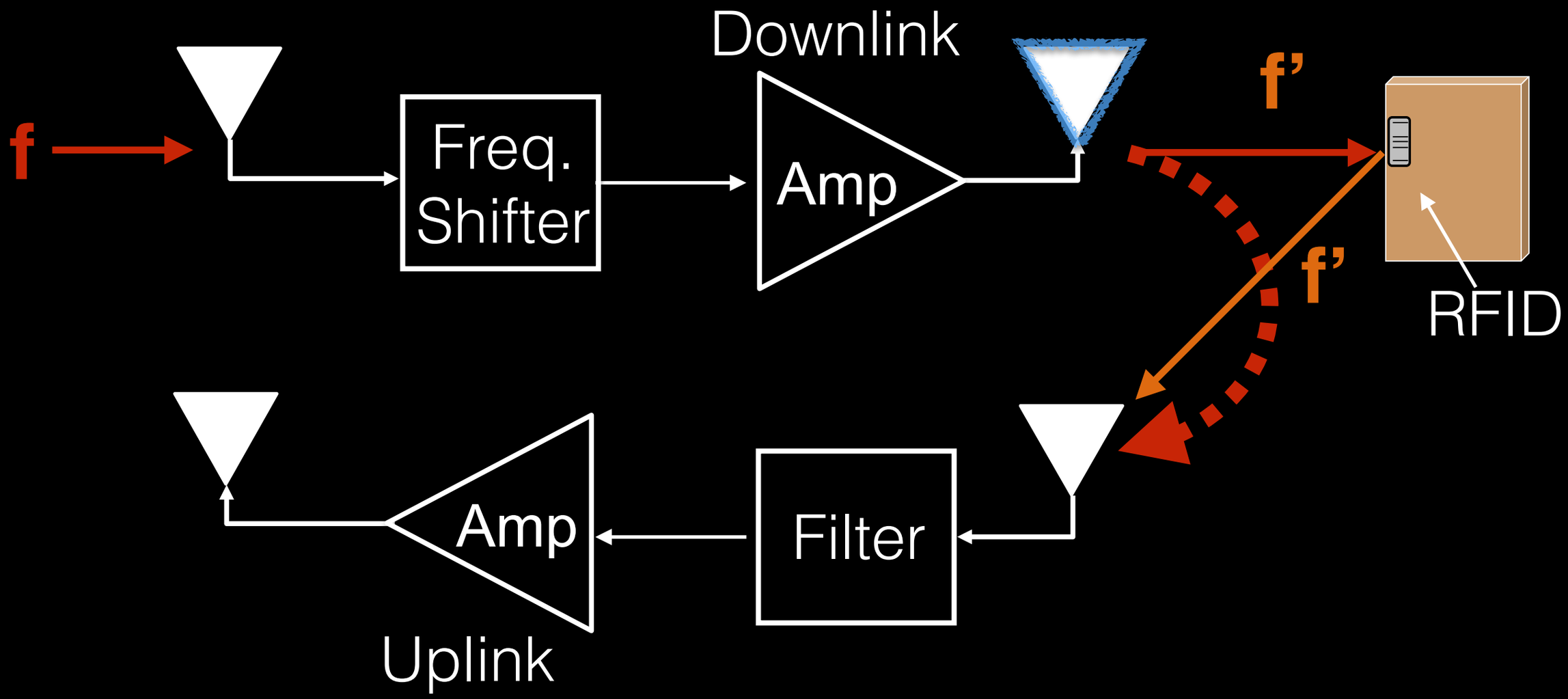


Use filtering in order to preserve RFID's response but eliminate self-interference

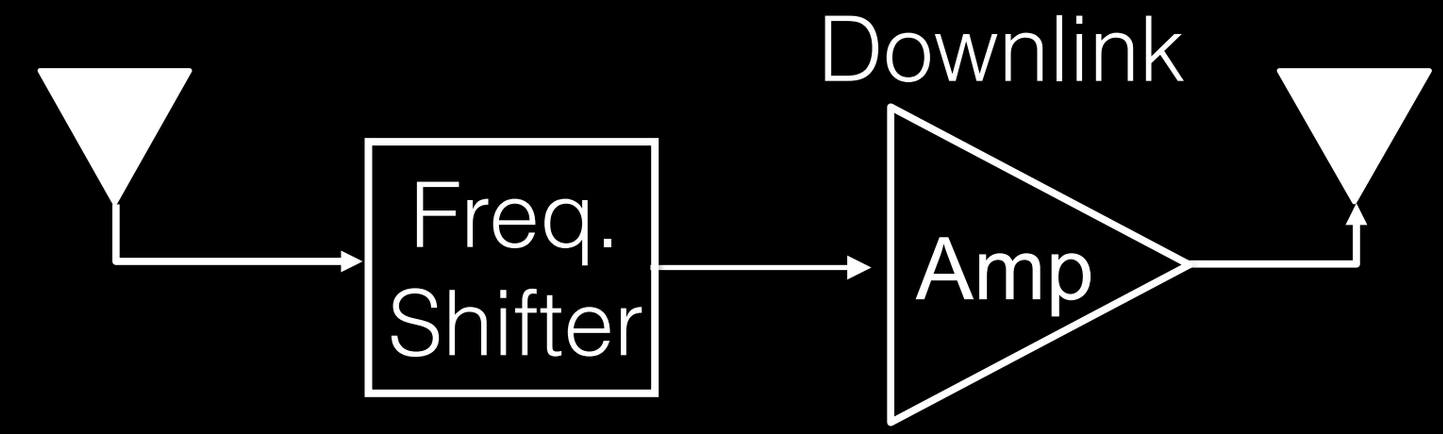
Use filtering in order to preserve RFID's response but eliminate self-interference

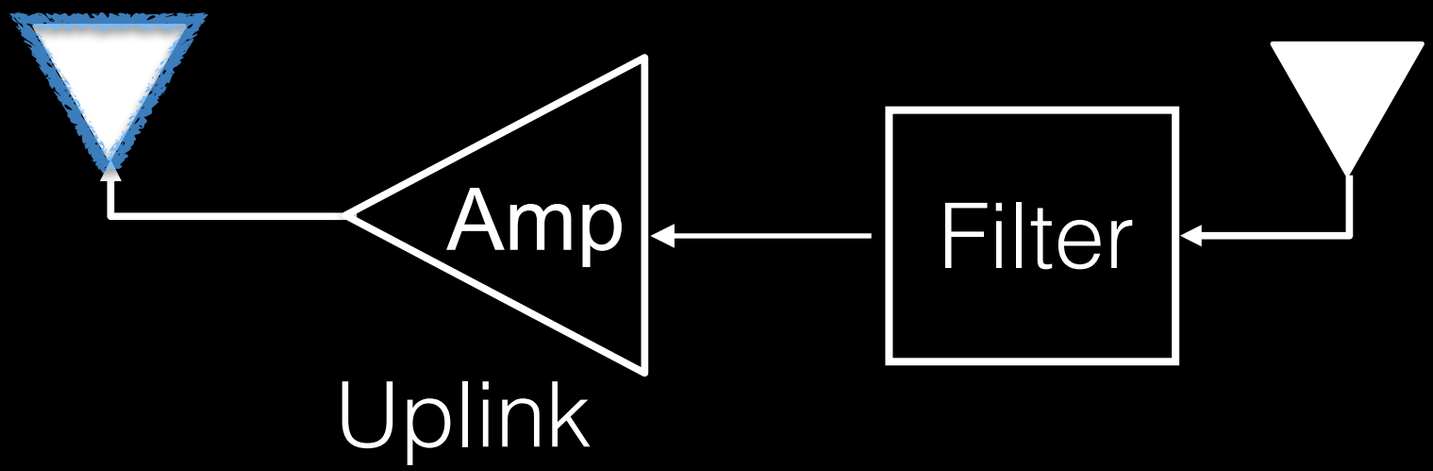


Use filtering in order to preserve RFID's response but eliminate self-interference



Leverage the same techniques on the uplink

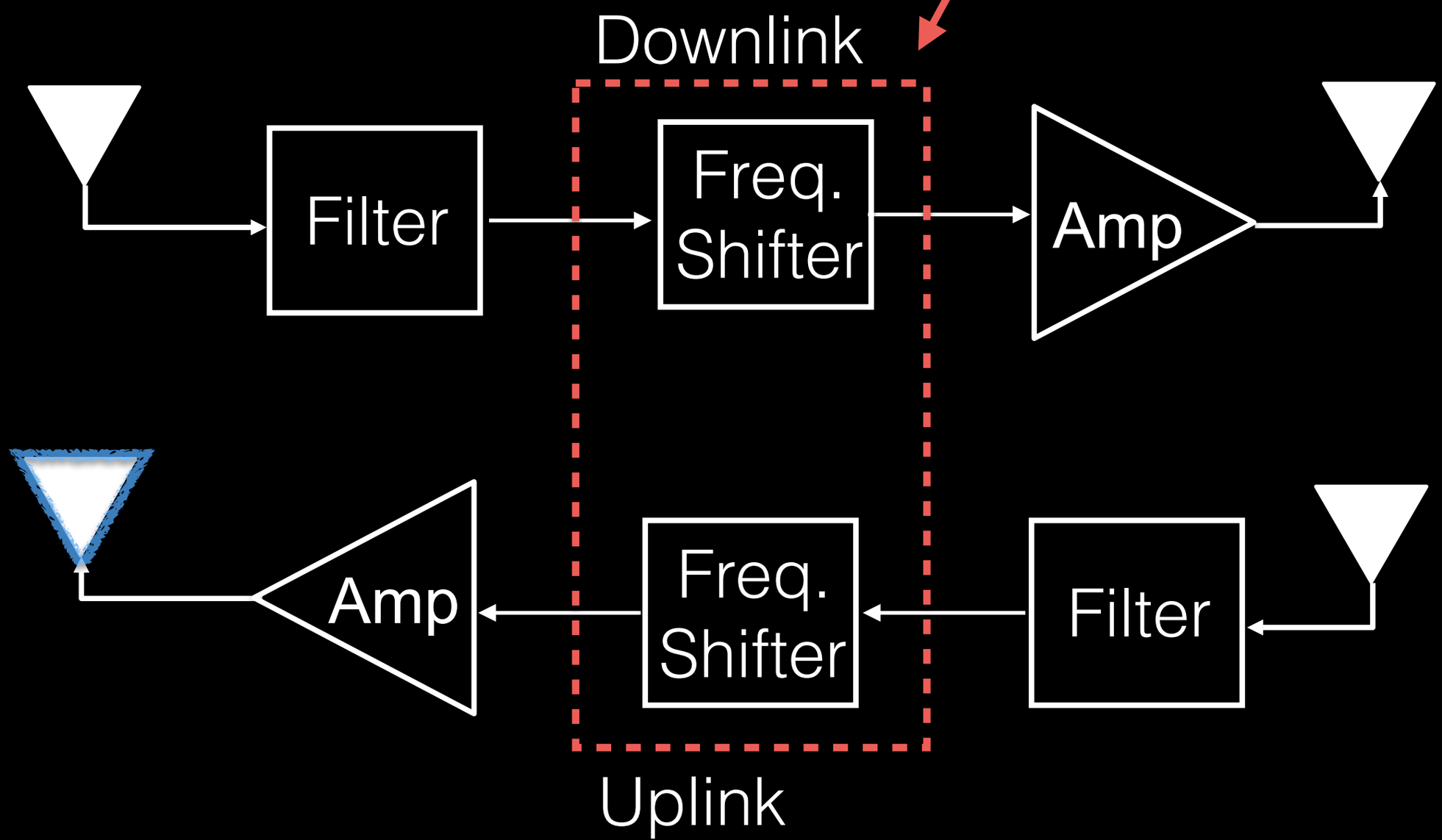




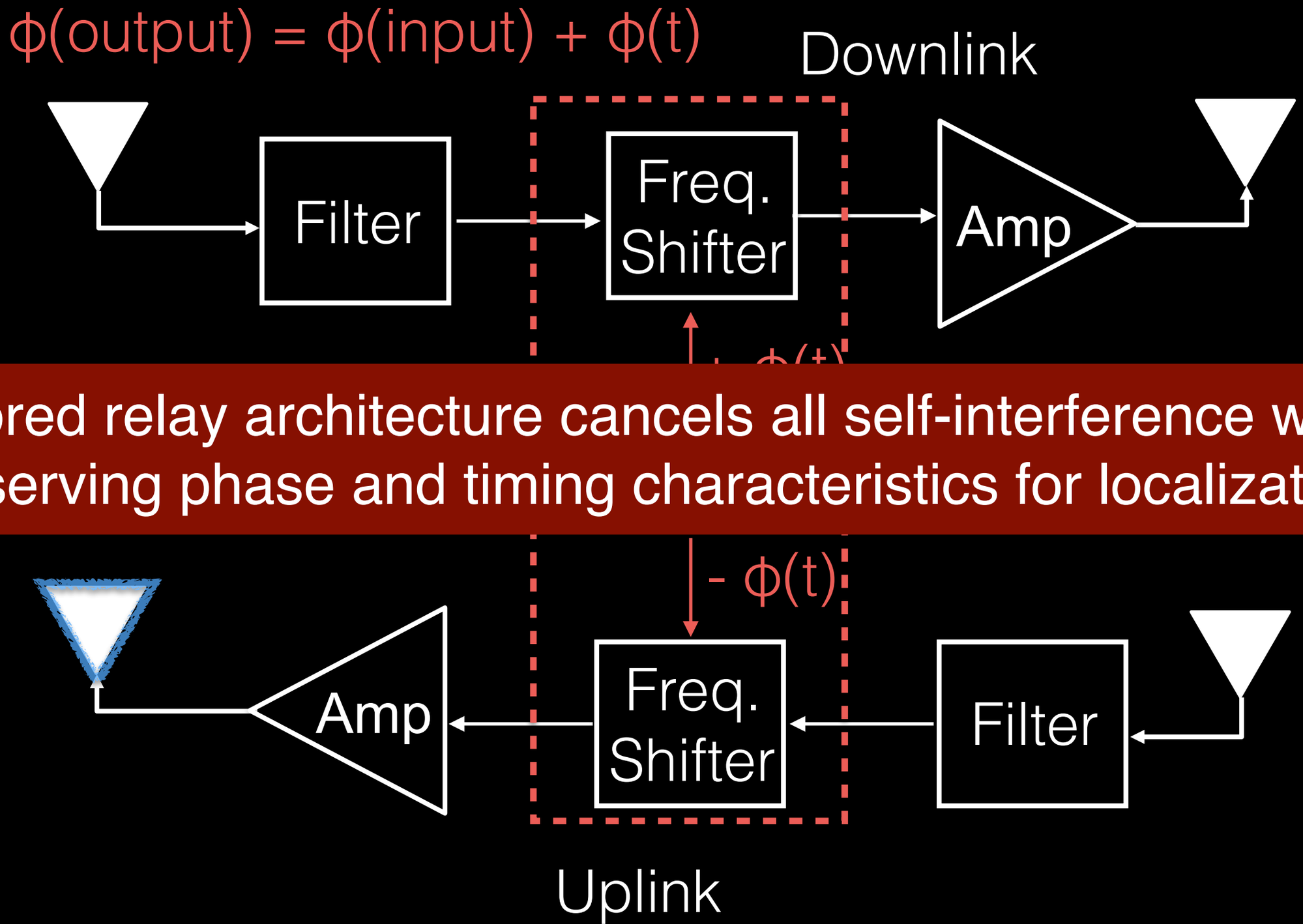
Leverage the same techniques on the uplink

Frequency shifting distorts phase information due to Carrier Frequency Offset (CFO)

$\phi(\text{output}) = \phi(\text{input}) + \phi'(t)$



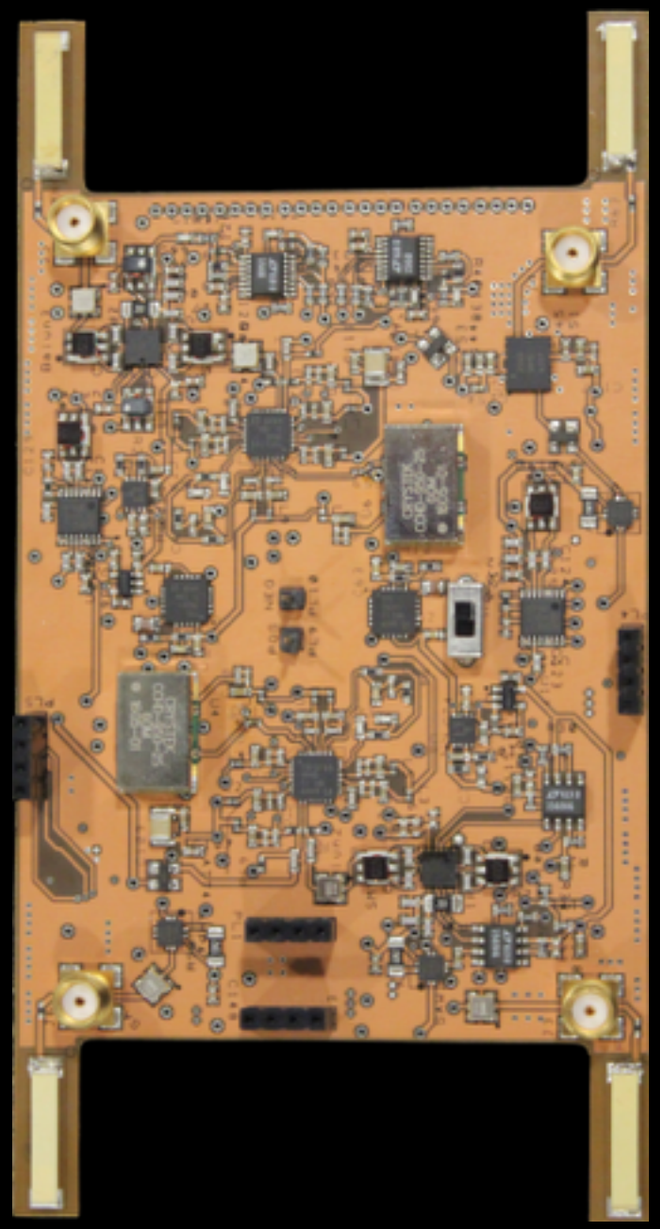
Exploit that we have control over both uplink and downlink



Mirrored relay architecture cancels all self-interference while preserving phase and timing characteristics for localization

Implementation & Evaluation

Implementation

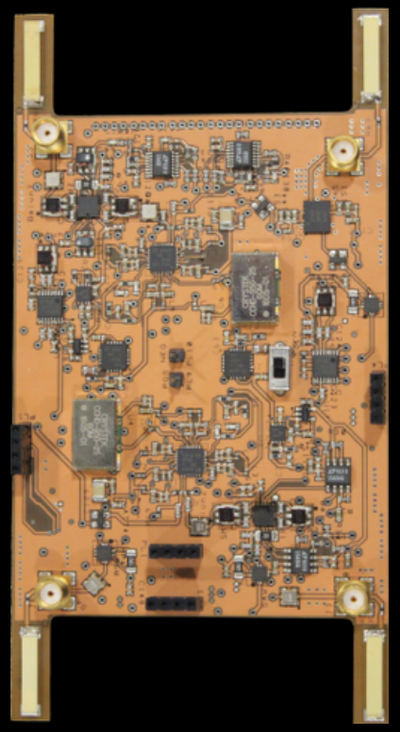


- PCB Board:4-layer FR4
- Size: 10 x 7.5 cm
- Weight: 35 g

Low power:

<3% of drone battery power

Implementation

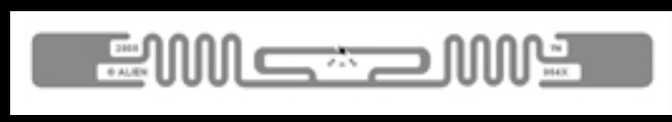


- PCB Board:4-layer FR4
- Size: 10 x 7.5 cm
- Weight: 35 g

- Parrot bebop-2
- Payload: 200 g

- RFID reader implemented using USRP N210 software radios
  - EPC-gen2 protocol

- Off-the-shelf battery-free RFIDs

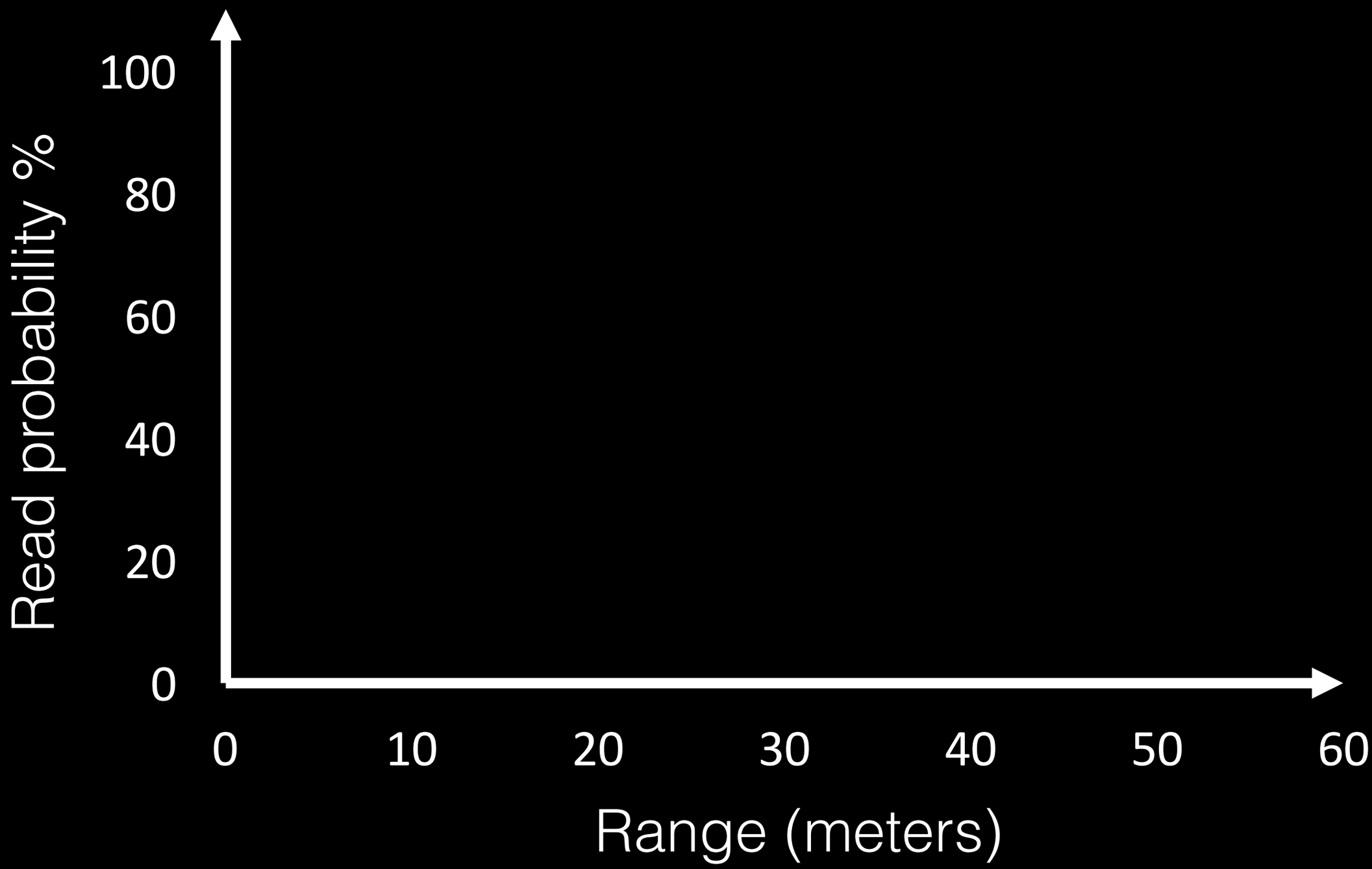


Evaluation

- Evaluated in different indoor environments
  - Fully-furnished with tables, chairs, computers, etc.
  - Test in line-of-sight and non-line-of-sight settings
- Ground truth: OptiTrack system
  - Infrared-based system that relies on visual markers
  - Achieves sub-centimeter accuracy
  - Operates only in line of sight

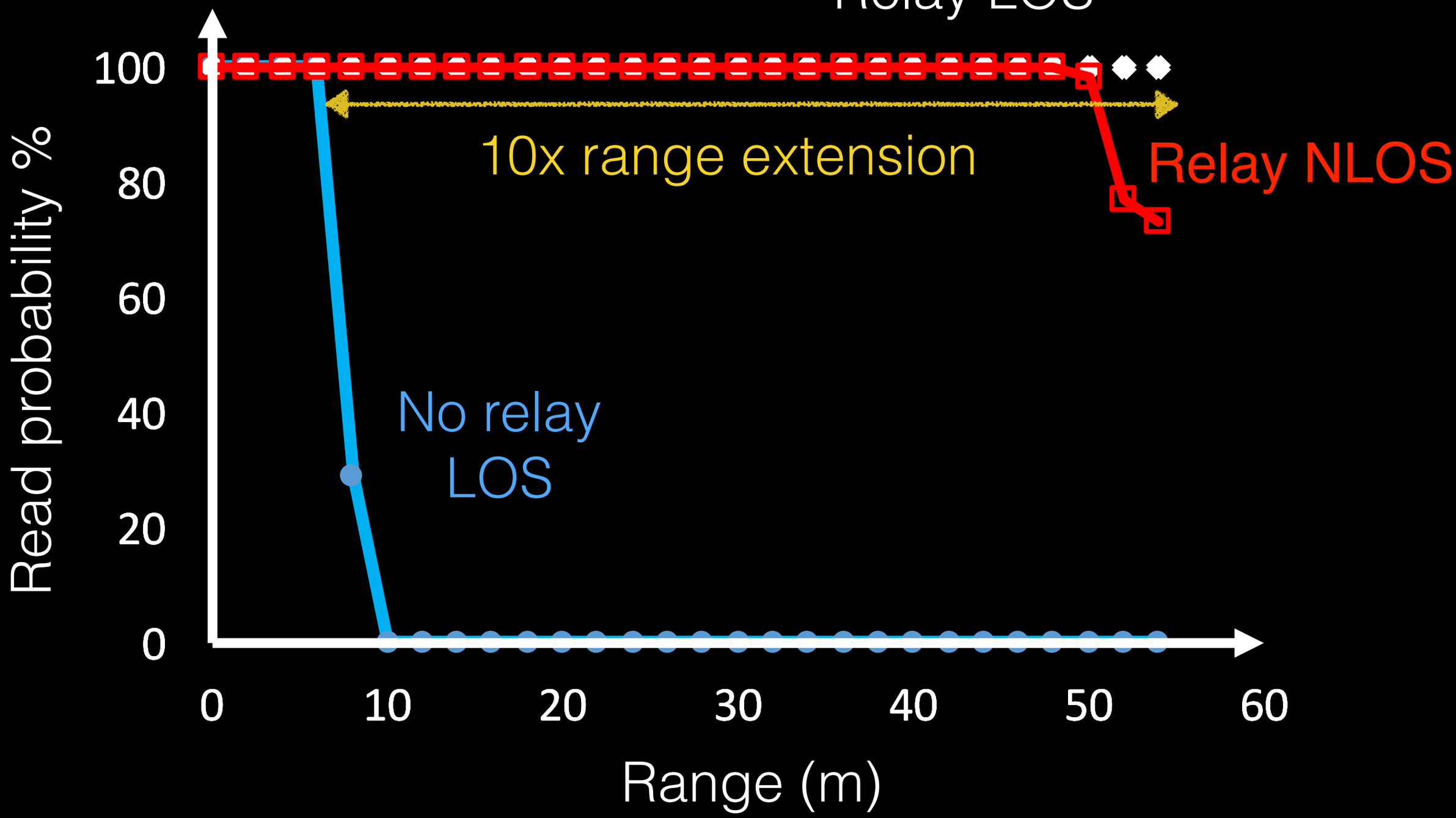
How much can RFly extend reading range?

100 experimental trials



How much can RFly extend reading range?

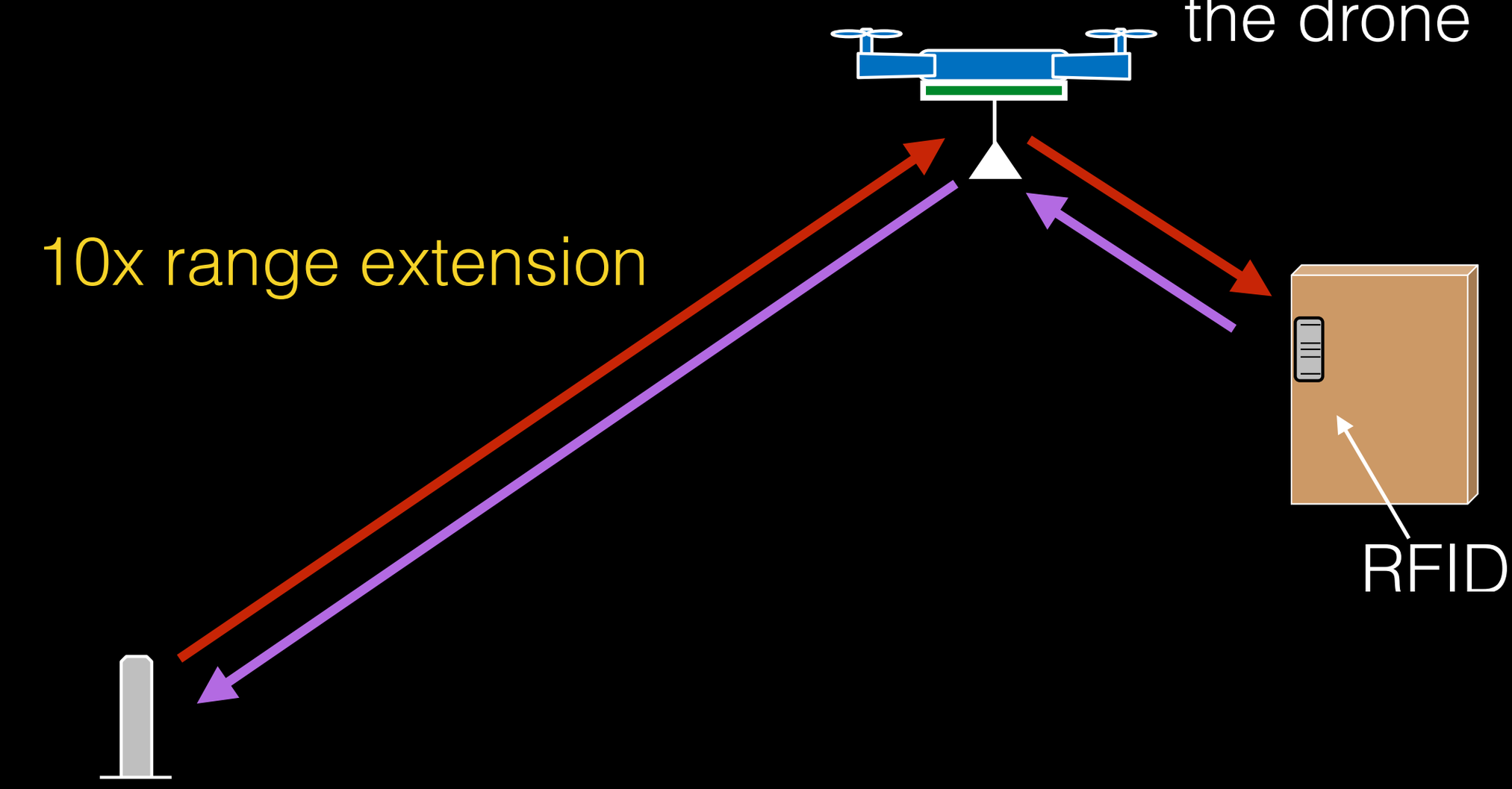
100 experimental trials



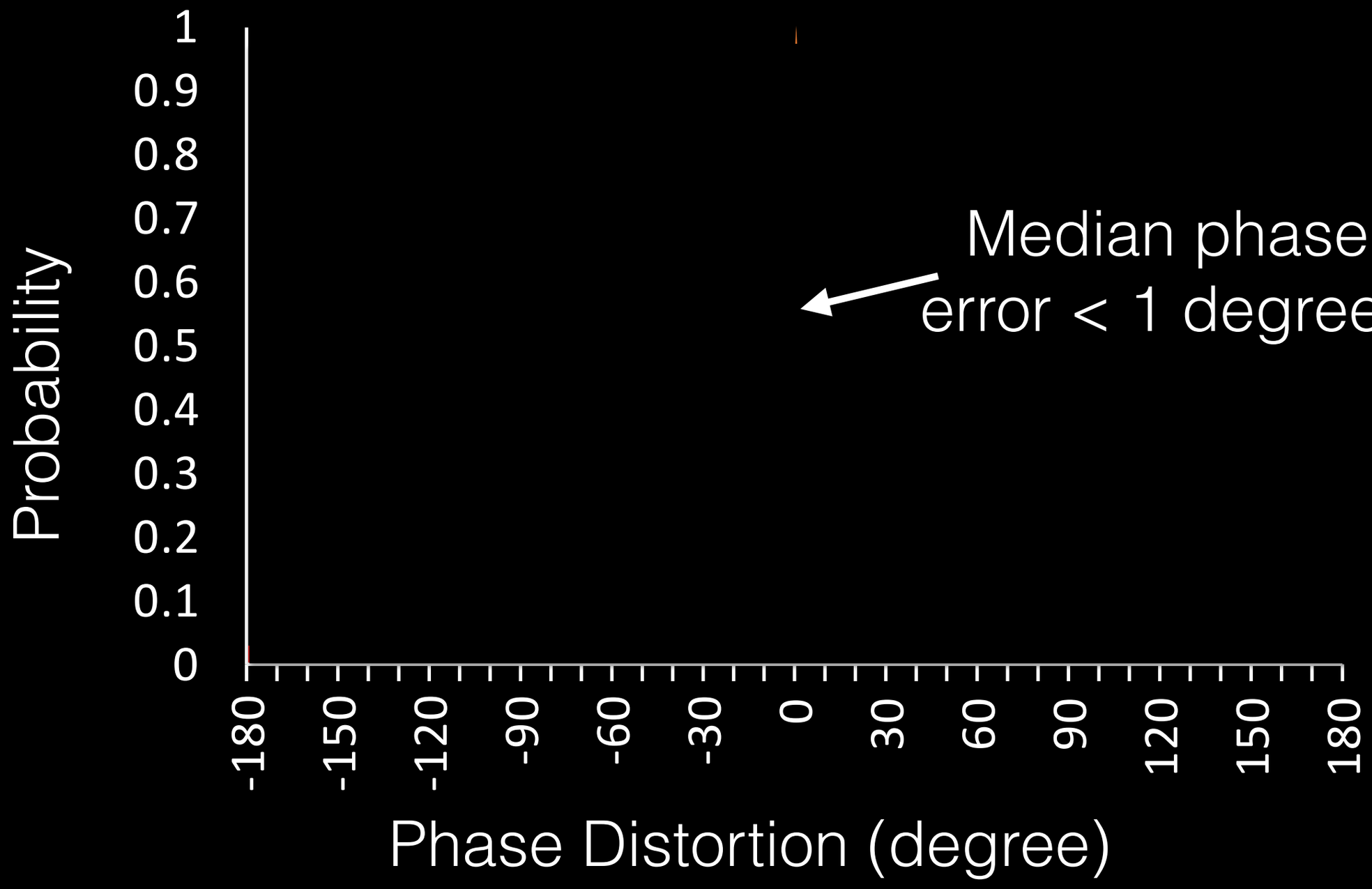
How much can RFly extend reading range?

100 experimental trials

Relay is powered up by the drone

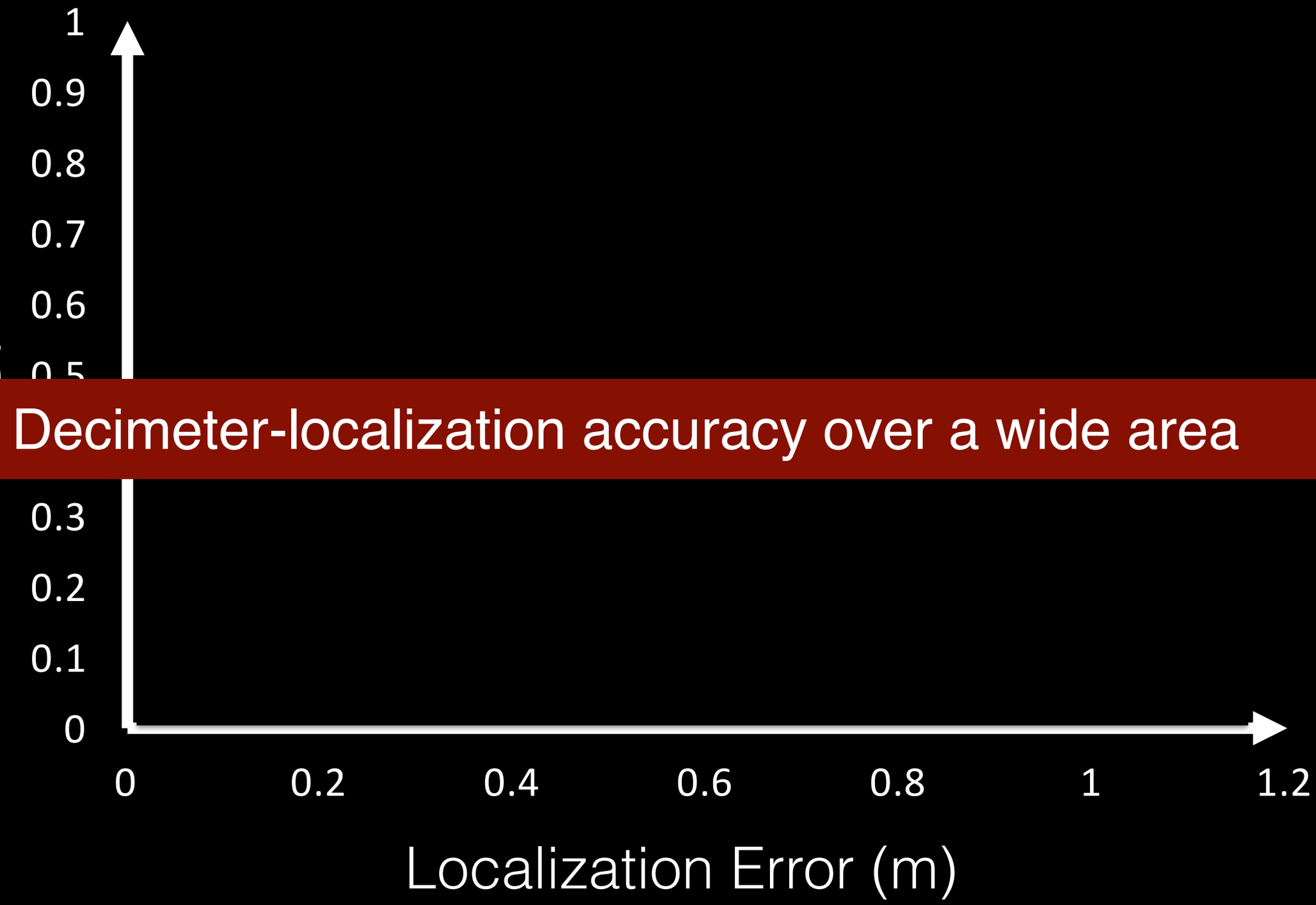


Does RFly preserve the phase for localization?



RFly's Localization Accuracy

100 experimental trials



Decimeter-localization accuracy over a wide area