RUHR UNIVERSITÄT BOCHUM

RUB

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

# Spatial-Domain Wireless Jamming with Reconfigurable Intelligent Surfaces

Philipp Mackensen[1]*, Paul Staat[2]*, Stefan Roth[1],

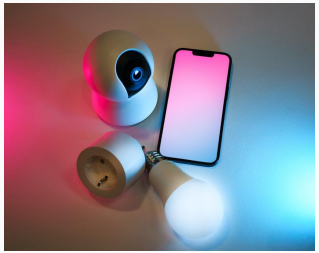
Aydin Sezgin[1], Christof Paar[2], and Veelasha Moonsamy[1]

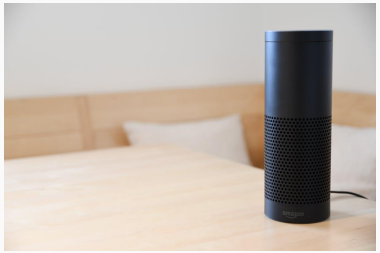
Network and Distributed System Security (NDSS) Symposium 2025
25th February 2025, San Diego, CA

[1] Ruhr University Bochum
[2] Max Planck Institute for Security and Privacy

* Equal contribution

# Ubiquitous Wireless Communication

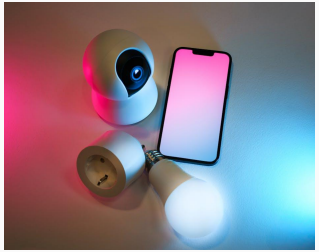



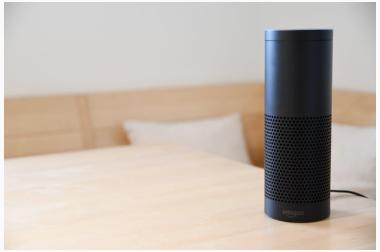


Open wireless medium makes devices vulnerable against **wireless jamming**!

Photos:
Daniel Aleksandersen, https://www.ctrl.blog/entry/review-asuswrt.html, Jakub Zerdzicki on pexels.com, Jens Mahnke on pexels.com, Fabian Hurnaus, pexels.com

# Ubiquitous Wireless Communication



Open wireless medium makes devices vulnerable against **wireless jamming**!

Los Angeles Times

CALIFORNIA

LAPD warns homeowners about a simple trick burglars use to disable home security systems

ring

Subscribers are Reading

FOR SUBSCRIBERS

Edison knew before Eaton fire that cutting power risked igniting blaze, records show

FOR SUBSCRIBERS

After this Australian town burned down, experts warned against rebuilding. Nobody listened

Evacuation warnings issued in burn zones as major rainstorm slams into L.A.

Feds won't test soil after L.A. wildfire cleanup, potentially leaving contamination behind

FOR SUBSCRIBERS

Photos:
Daniel Aleksandersen, https://www.ctrl.blog/entry/review-asuswrt.html, Jakub Zerdzicki on pexels.com, Jens Mahnke on pexels.com, Fabian Hurnaus, pexels.com

# Why we Need to Revisit Wireless Jamming

- Long-standing and well-studied topic in wireless security

# Why we Need to Revisit Wireless Jamming

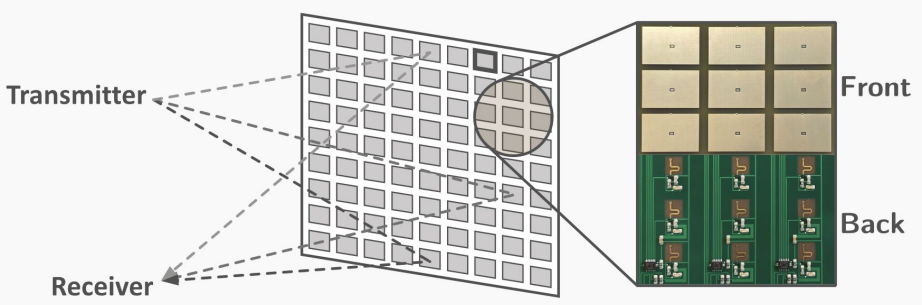
- Long-standing and well-studied topic in wireless security
- Threat exploration must continue to keep up with recent technological advancements

# Why we Need to Revisit Wireless Jamming

- Long-standing and well-studied topic in wireless security
- Threat exploration must continue to keep up with recent technological advancements
- **This work:**
  **Wireless jamming in view of emerging Reconfigurable Intelligent Surface (RIS) technology**

# Reconfigurable Intelligent Surface (RIS) 101

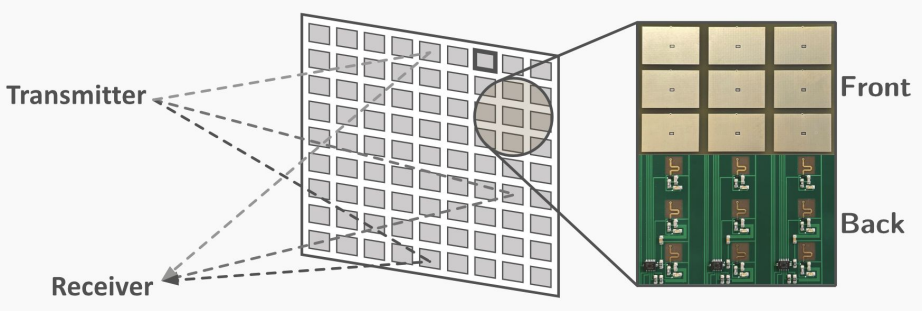
- **Smart radio environments**
  - Optimize wireless communication channel



# Reconfigurable Intelligent Surface (RIS) 101

- **Smart radio environments**
  - Optimize wireless communication channel

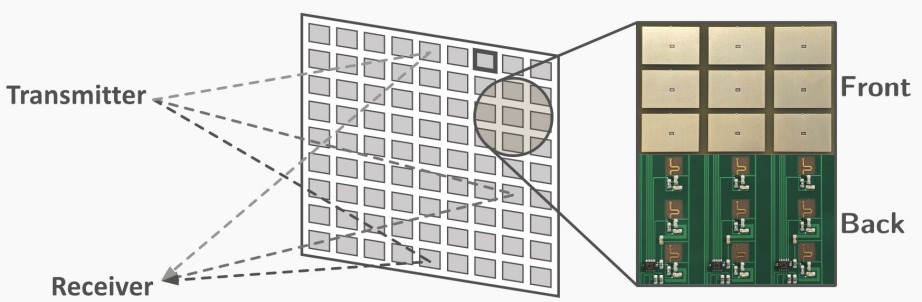
- Digital control over the surface reflection properties
  - Many individually adjustable reflective elements



# Reconfigurable Intelligent Surface (RIS) 101

- **Smart radio environments**
  - Optimize wireless communication channel

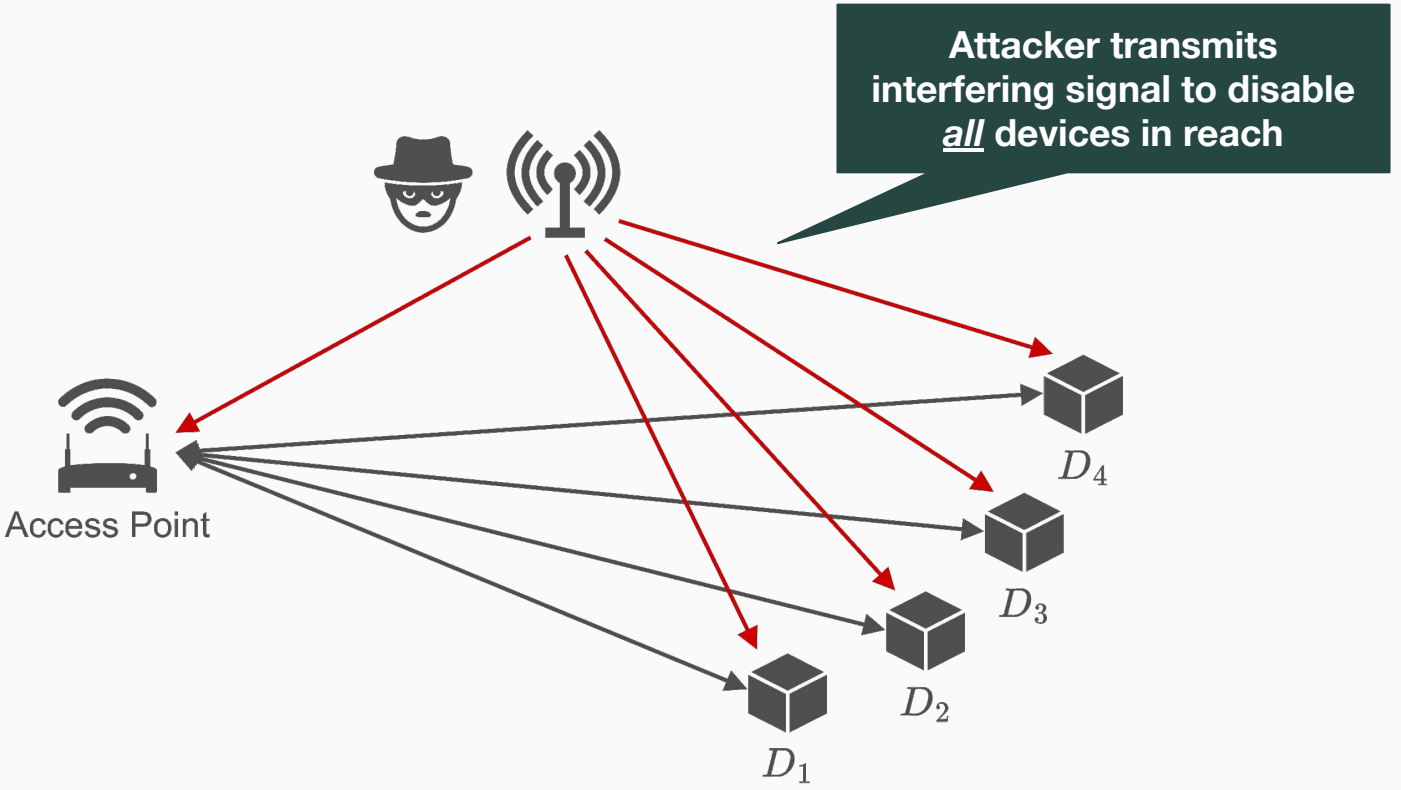
- Digital control over the surface reflection properties
  - Many individually adjustable reflective elements



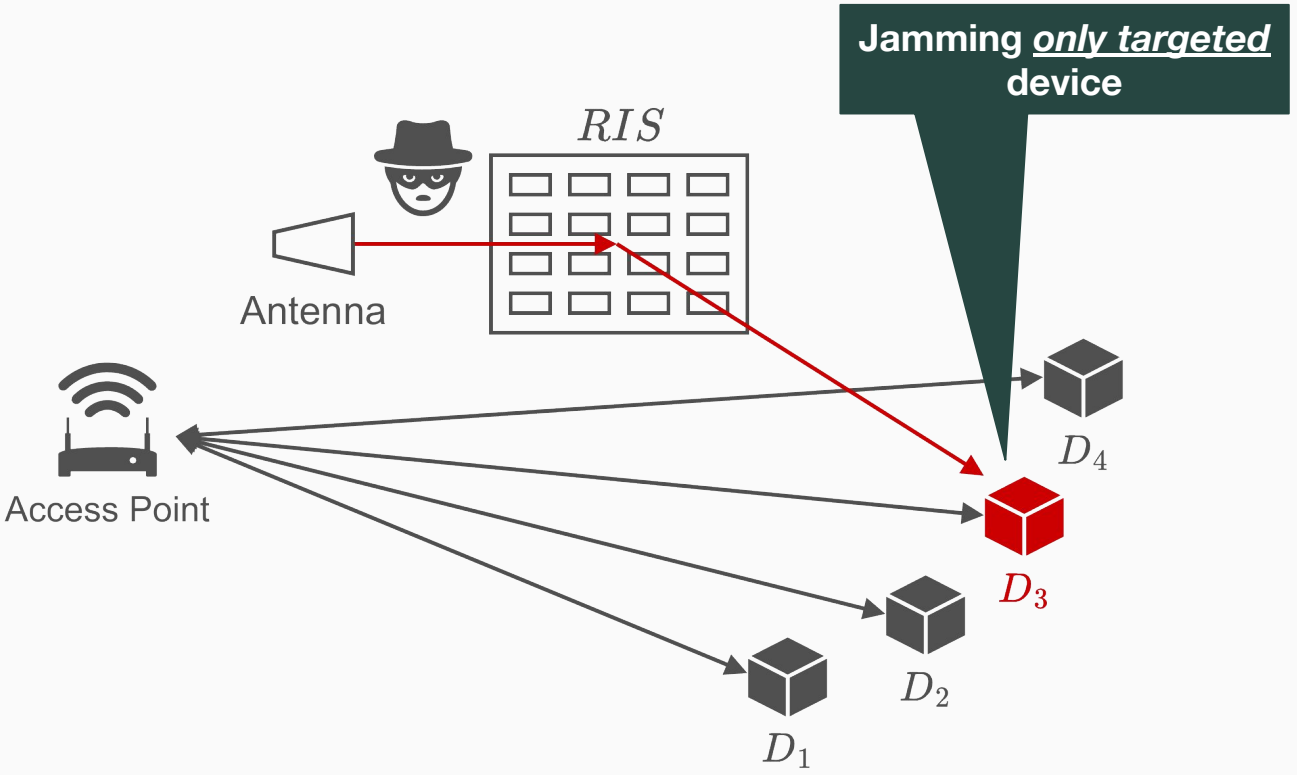

- Implemented as a low-cost printed circuit board[1]

[1] https://github.com/mheinri/OpenSourceRIS

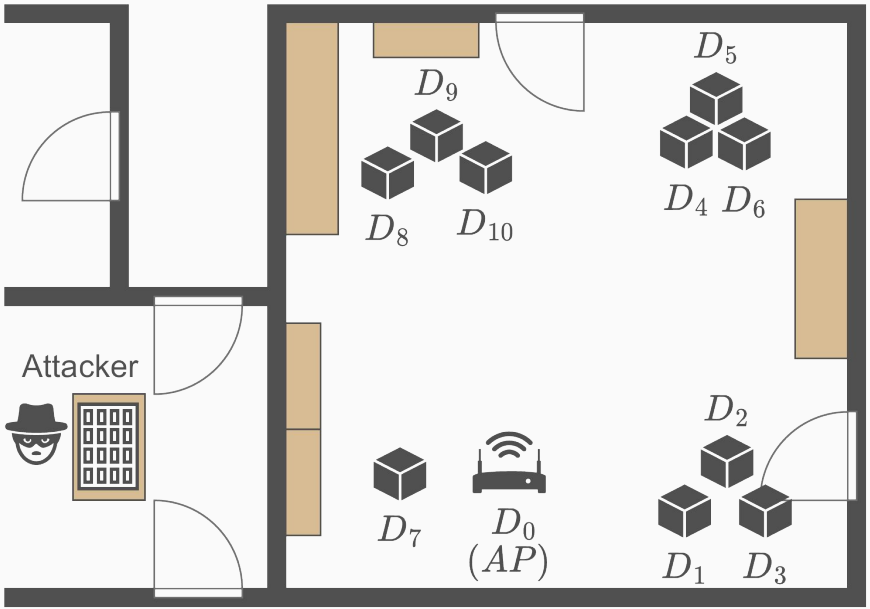
# Classical Jamming Attacks



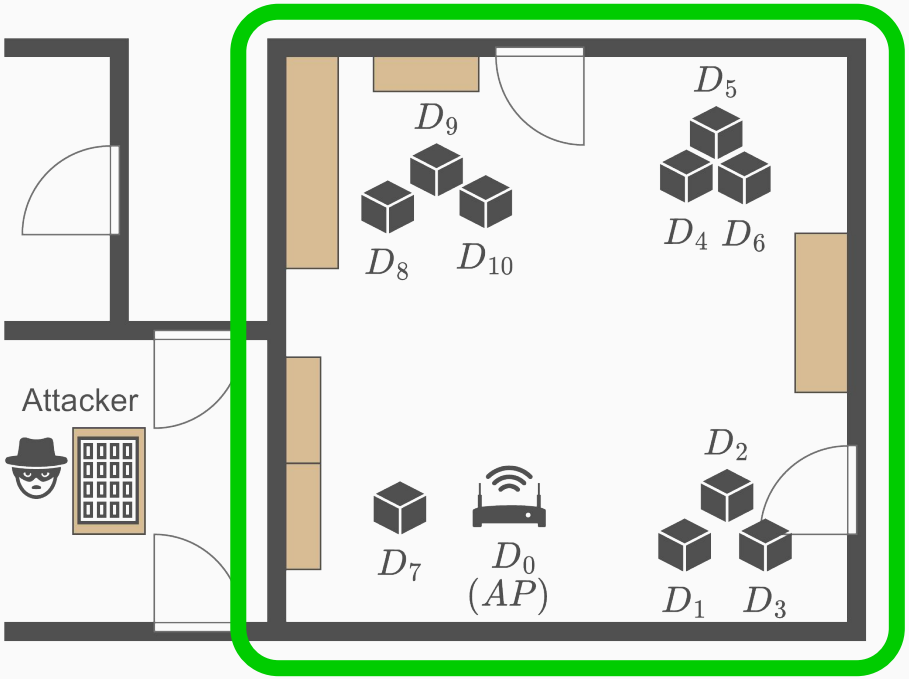
# RIS enables Spatially Selective Jamming



# Experimental Setup



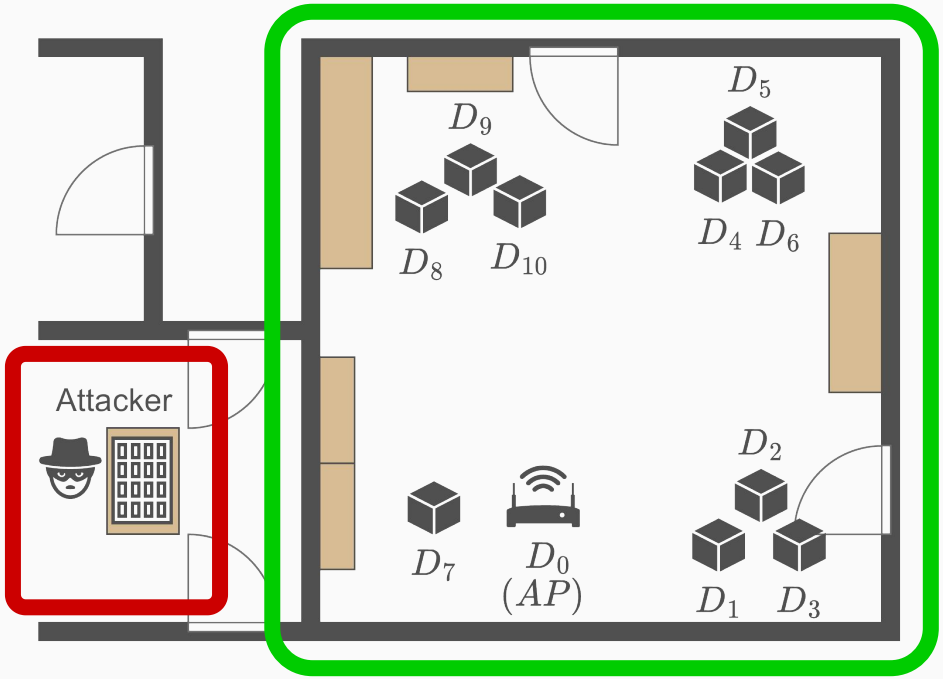
# Experimental Setup




## Victim Wi-Fi network

- Access point (AP)
- 10 x Raspberry Pi

# Experimental Setup

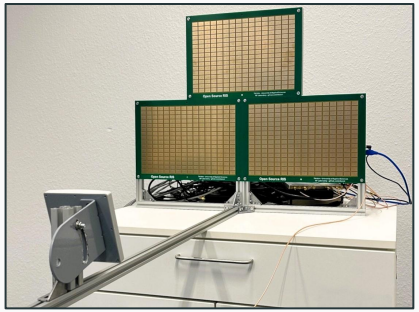



## Victim Wi-Fi network

- Access point (AP)
- 10 x Raspberry Pi

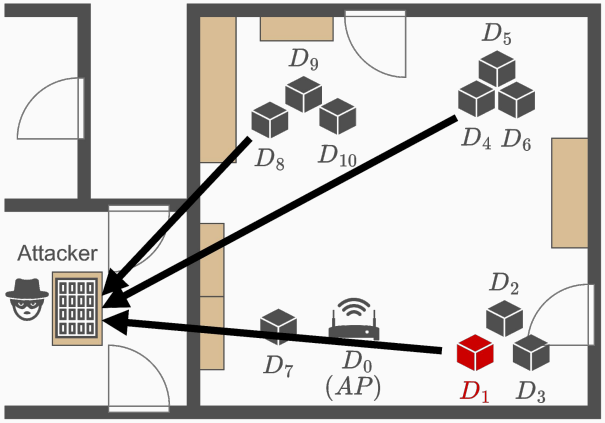
## Attacker

- Directional antenna facing RIS



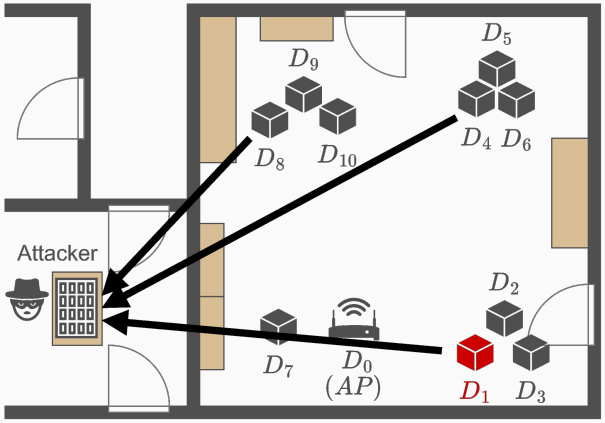
# Attack Strategy (1/2): Adapt RIS Configuration

- **Passive eavesdropping** of wireless environment



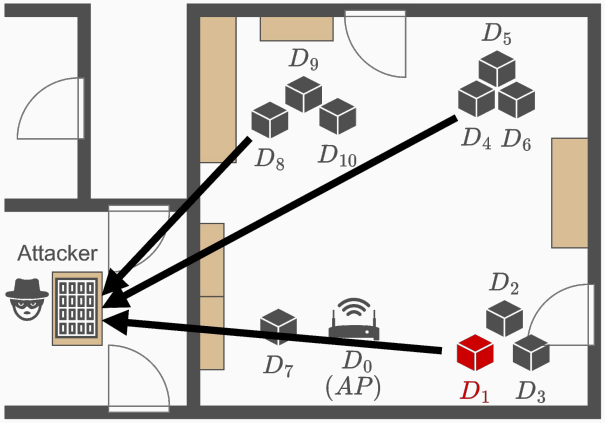
# Attack Strategy (1/2): Adapt RIS Configuration

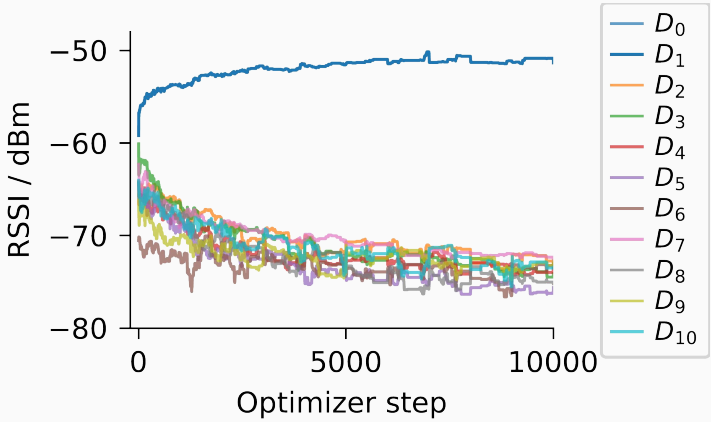
- **Passive eavesdropping** of wireless environment
- Adapt RIS configuration



# Attack Strategy (1/2): Adapt RIS Configuration

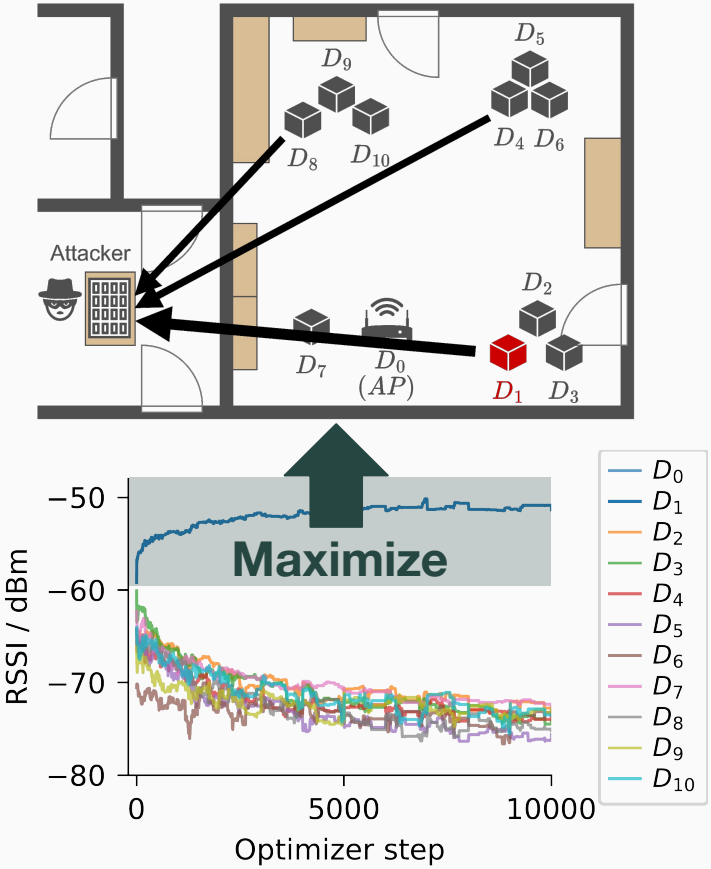
- **Passive eavesdropping** of wireless environment
- Adapt RIS configuration
- Shape received signal strengths:



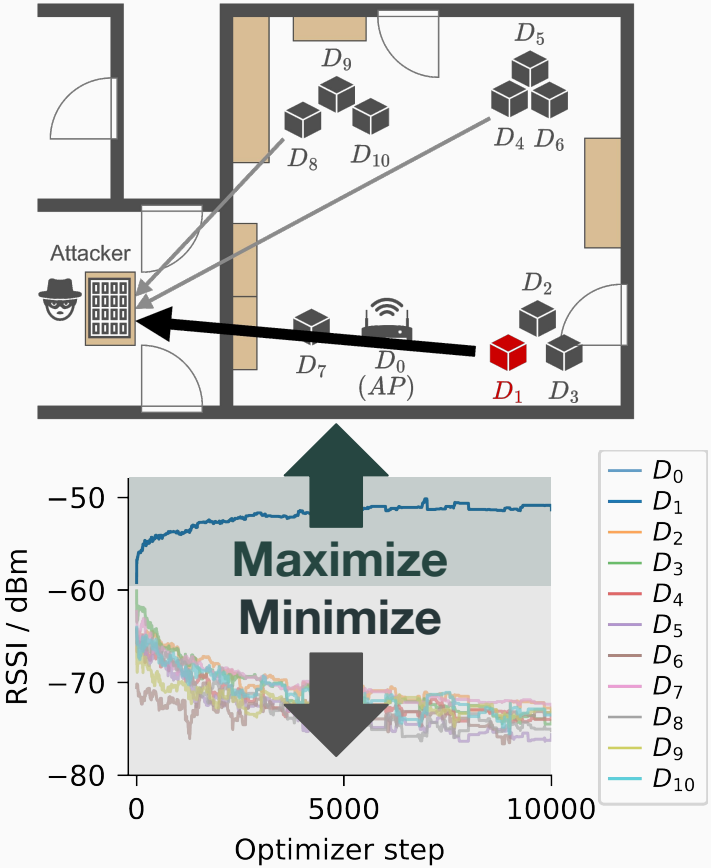
# Attack Strategy (1/2): Adapt RIS Configuration

- **Passive eavesdropping** of wireless environment
- Adapt RIS configuration
- Shape received signal strengths:
  - Maximize jamming **target**



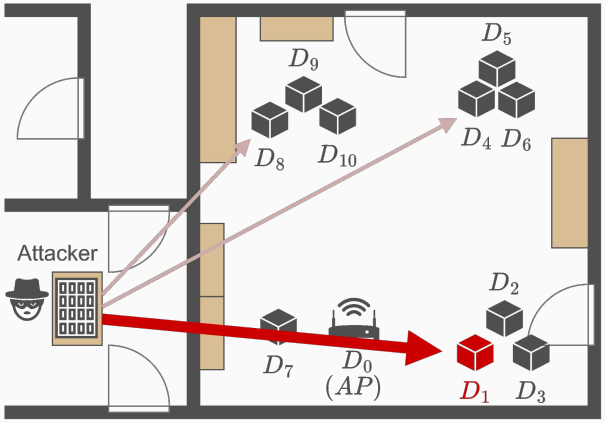
# Attack Strategy (1/2): Adapt RIS Configuration

- **Passive eavesdropping** of wireless environment
- Adapt RIS configuration
- Shape received signal strengths:
  - Maximize jamming **target**
  - Minimize others



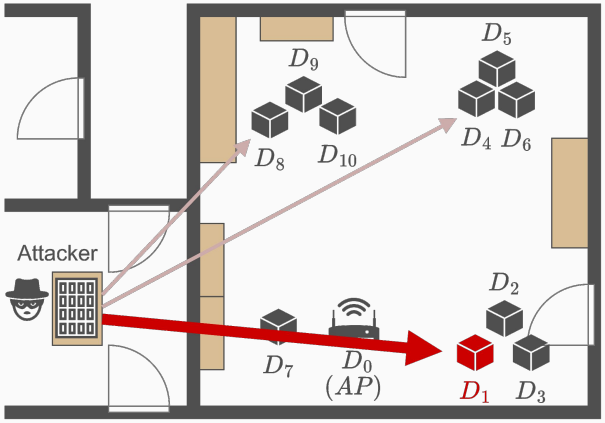
# Attack Strategy (2/2): Active Jamming

- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*



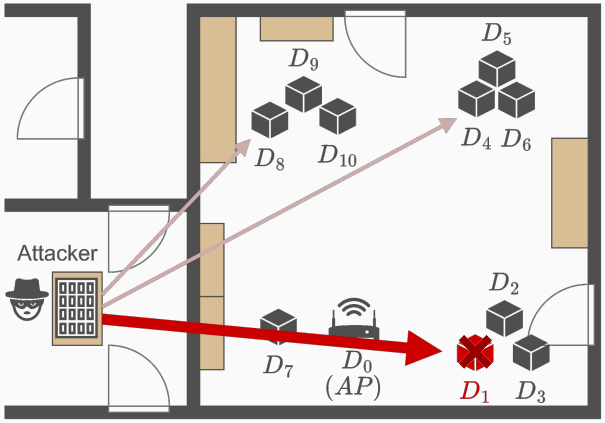
# Attack Strategy (2/2): Active Jamming

- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*
- Use previously adapted RIS configuration to transmit jamming signal



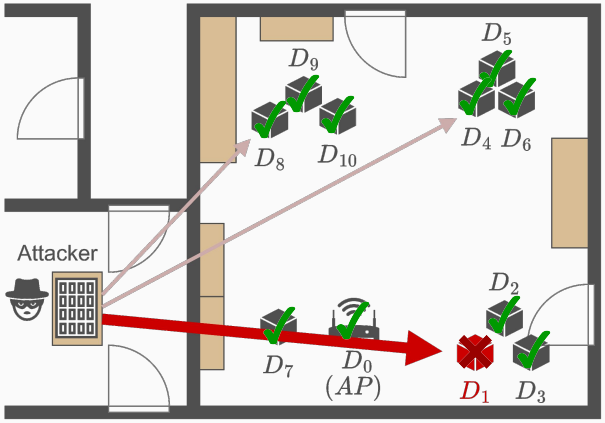
# Attack Strategy (2/2): Active Jamming

- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*
- Use previously adapted RIS configuration to transmit jamming signal
- Target device is jammed



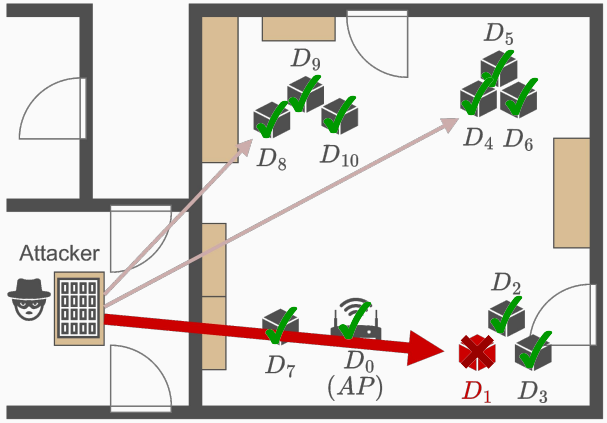
# Attack Strategy (2/2): Active Jamming

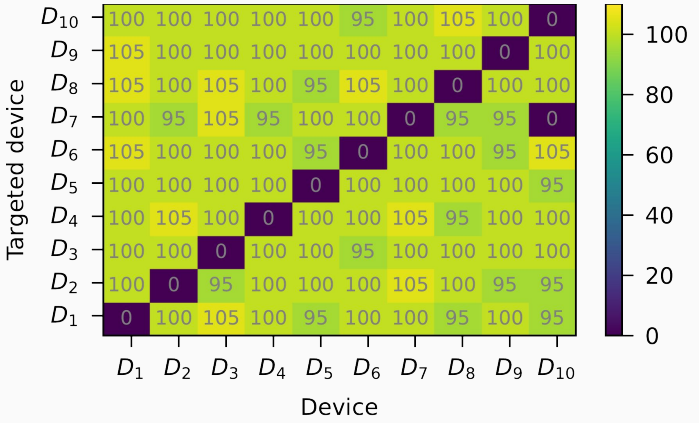
- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*
- Use previously adapted RIS configuration to transmit jamming signal
- Target device is jammed
- Others remain operational



# Attack Strategy (2/2): Active Jamming

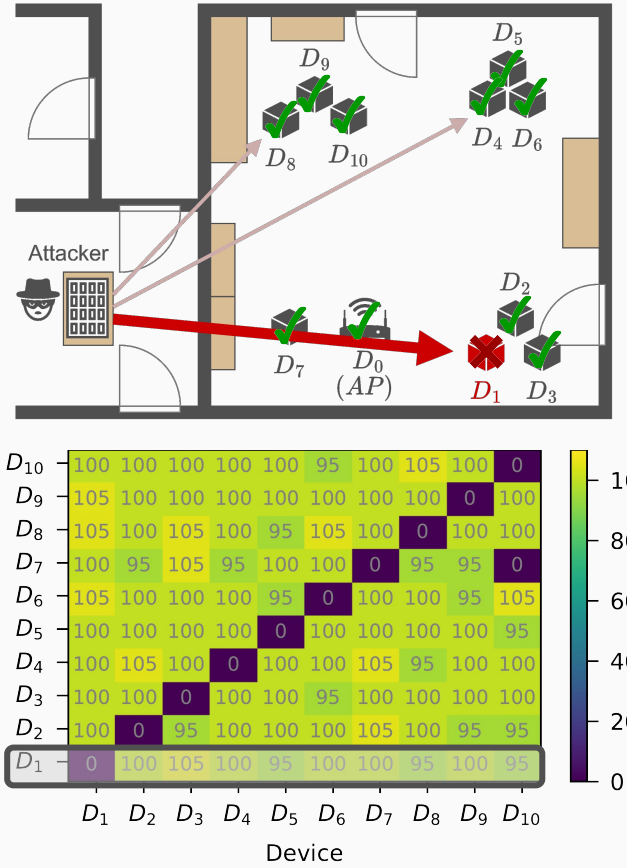
- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*
- Use previously adapted RIS configuration to transmit jamming signal
- Target device is jammed
- Others remain operational



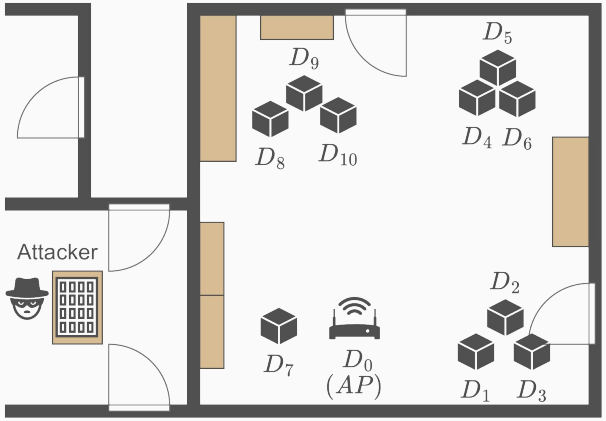
# Attack Strategy (2/2): Active Jamming

- Exploit reciprocal wireless channel:
  - Attacker's signal *transmission* behaves the same as *reception*
- Use previously adapted RIS configuration to transmit jamming signal
- Target device is jammed
- Others remain operational



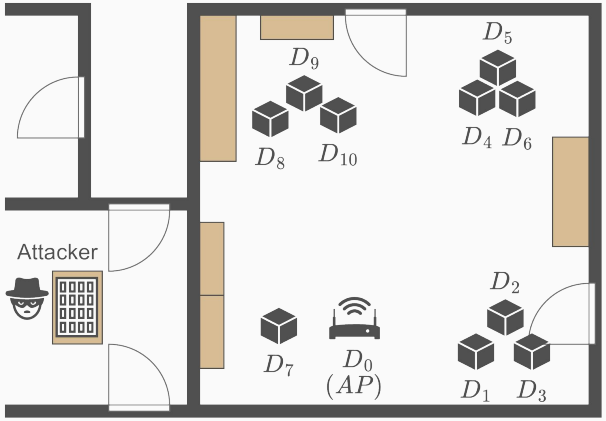
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices



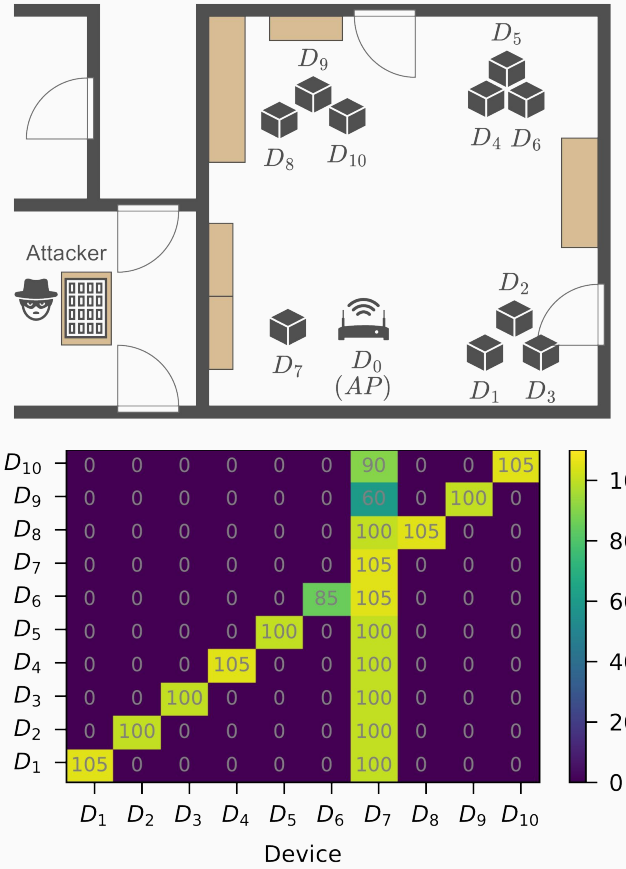
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device



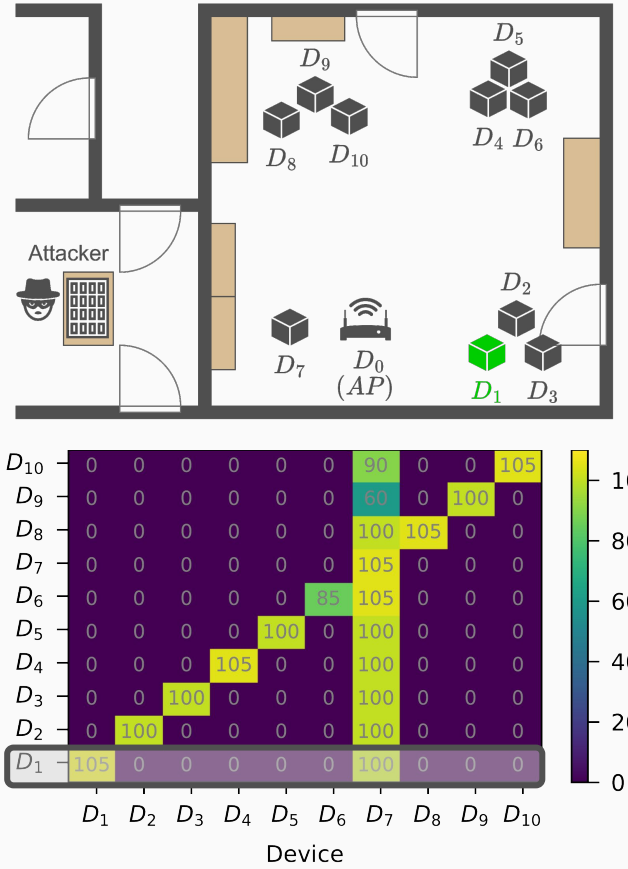
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device



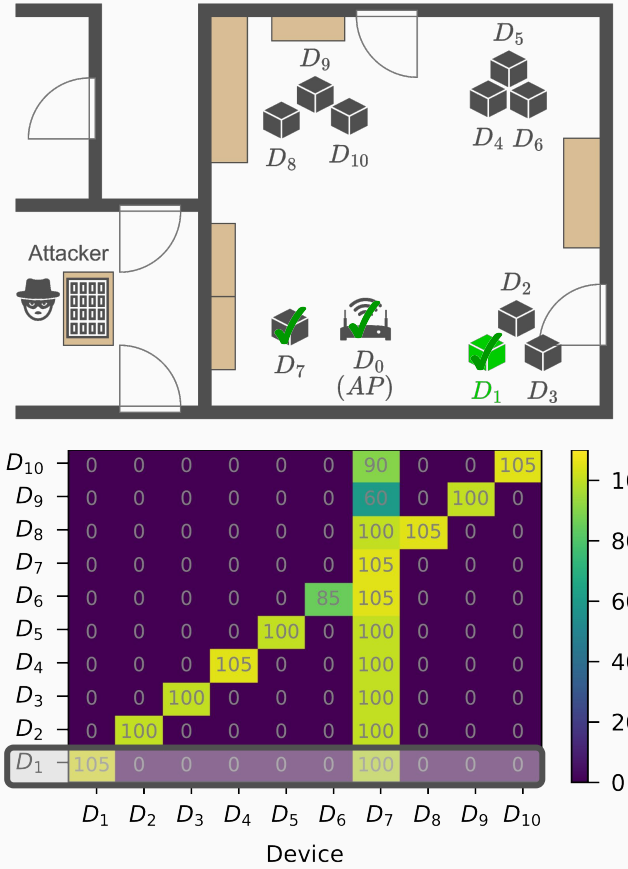
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device



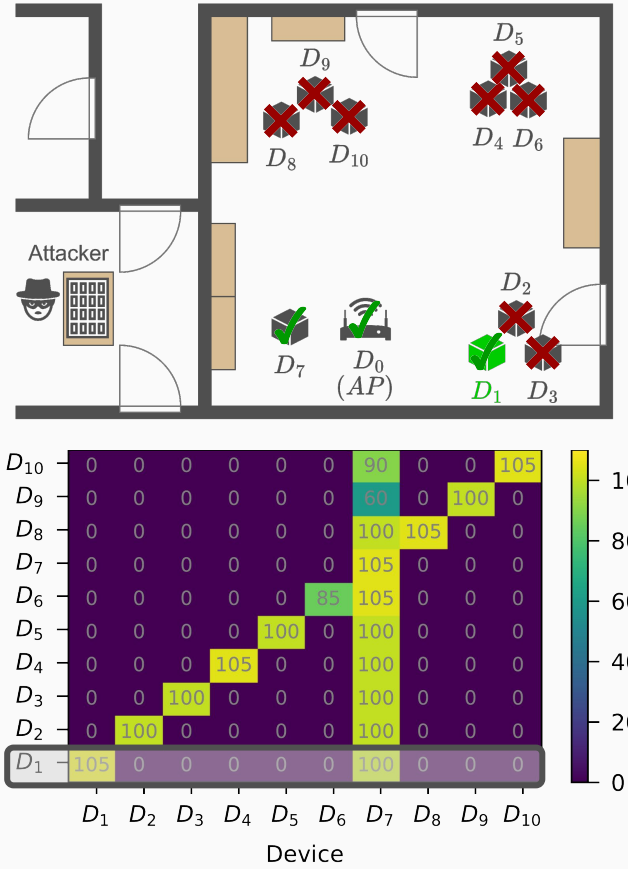
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device



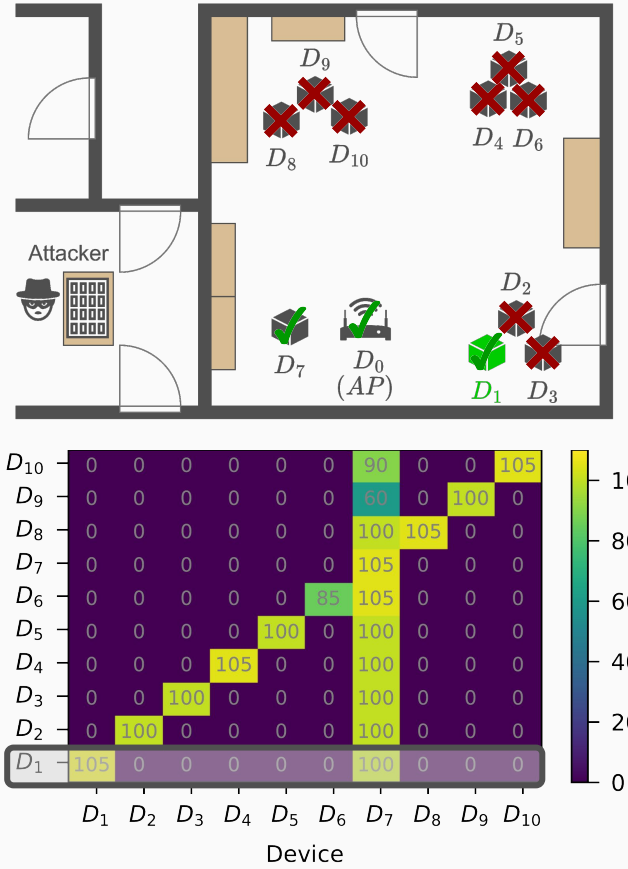
# Multi-Target Jamming

- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device

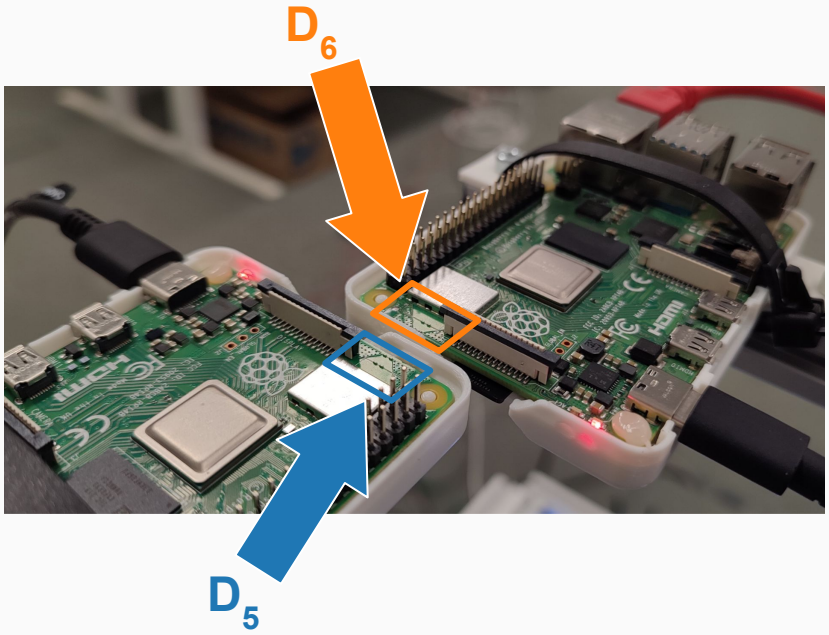


# Multi-Target Jamming

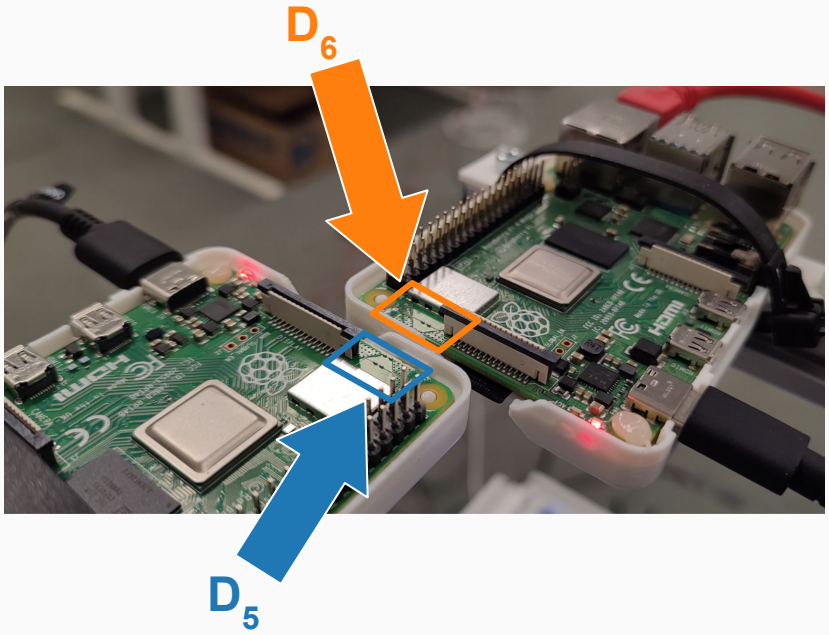
- Attack likewise works when targeting *multiple* devices
- Extreme case:
  - Jam all but one device
- $D_7$ hard to jam since it is close to the access point and enjoys a strong signal

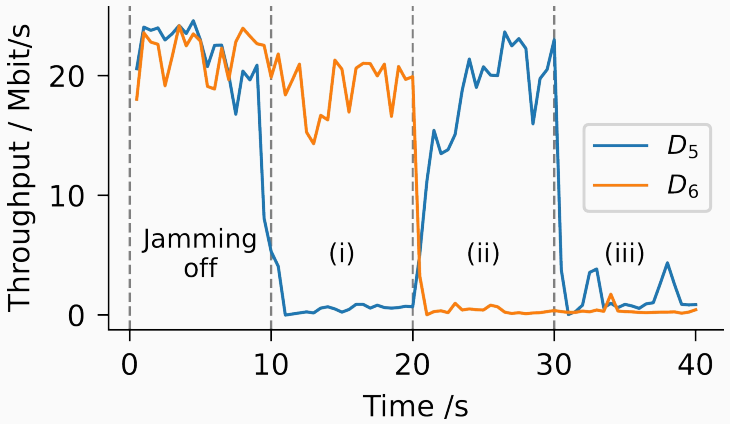


# Jamming Devices in Close Proximity

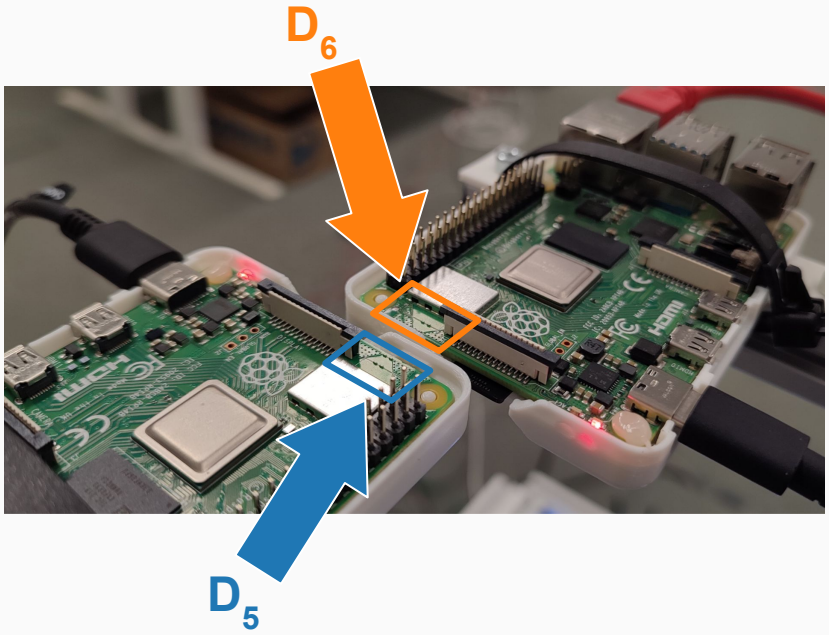


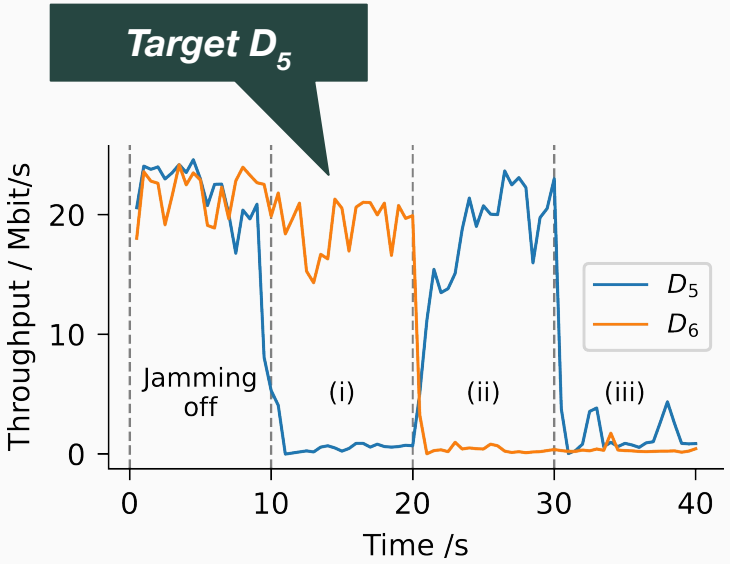
# Jamming Devices in Close Proximity



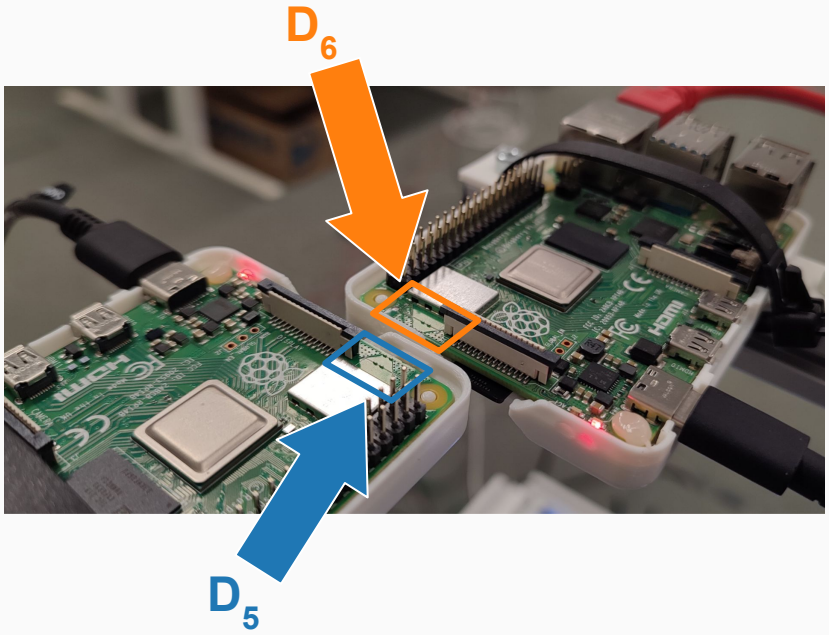



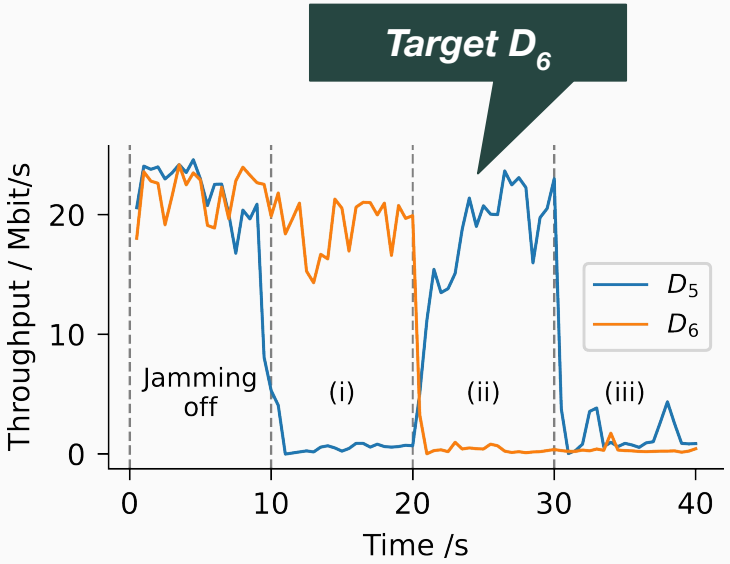
# Jamming Devices in Close Proximity



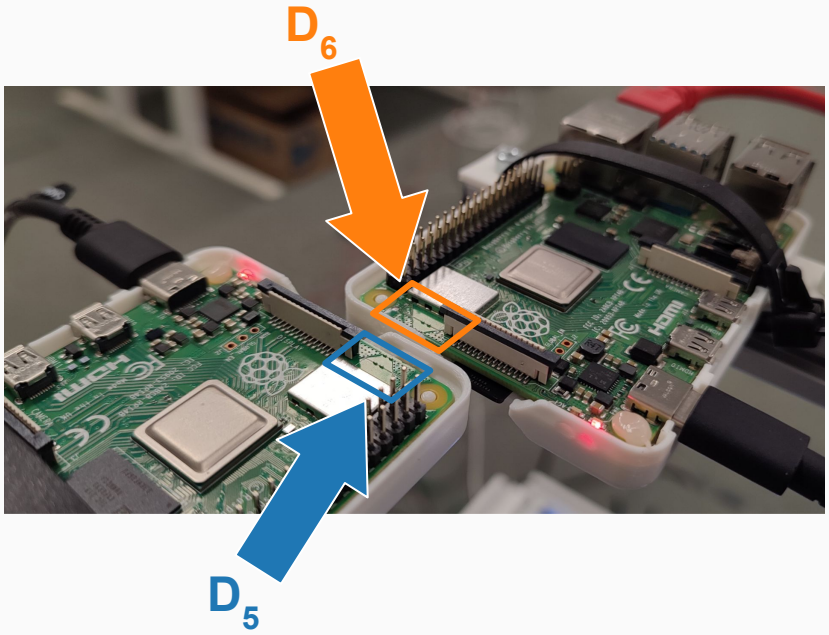



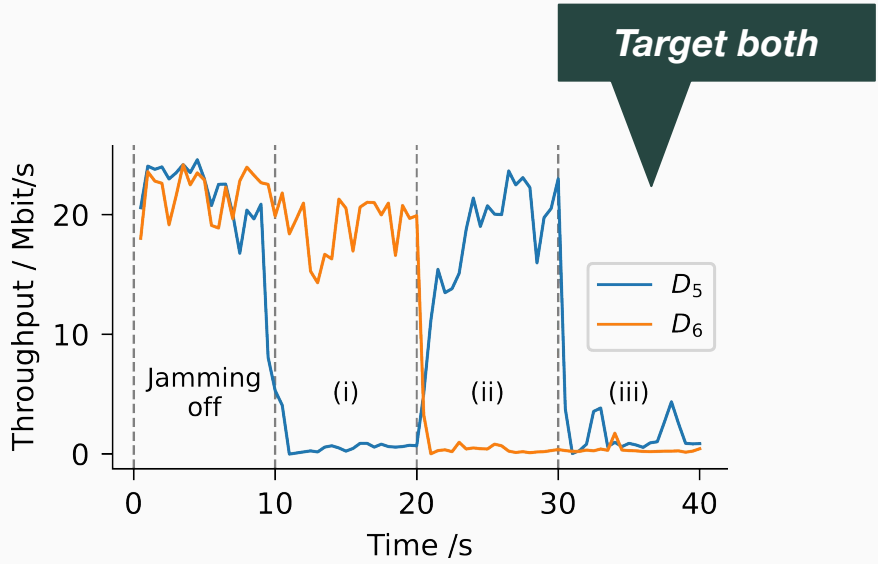
# Jamming Devices in Close Proximity



# Jamming Devices in Close Proximity

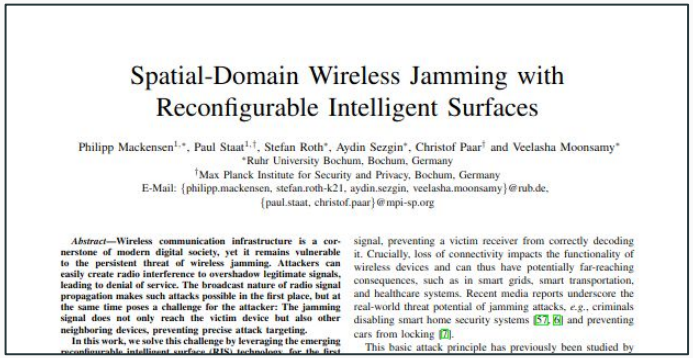



- Attack still works even when devices are very close to each other
- Dynamic attack target selection through RIS configuration switching

# Summary and Conclusion

- Vivid example for threat potential of RIS technology:
  - Spatially-selective jamming attacks
- Significantly lowers the bar for sophisticated jamming attackers



Spatial-Domain Wireless Jamming with Reconfigurable Intelligent Surfaces

Philipp Mackensen[1,*], Paul Staat[1,†], Stefan Roth*, Aydin Sezgin*, Christof Paar[†] and Veelasha Moonsamy*
*Ruhr University Bochum, Bochum, Germany
[†]Max Planck Institute for Security and Privacy, Bochum, Germany
E-Mail: {philipp.mackensen, stefan.roth-k21, aydin.sezgin, veelasha.moonsamy}@rub.de,
{paul.staat, christof.paar}@mpi-sp.org

***Abstract*—Wireless communication infrastructure is a cornerstone of modern digital society, yet it remains vulnerable to the persistent threat of wireless jamming. Attackers can easily create radio interference to overshadow legitimate signals, leading to denial of service. The broadcast nature of radio signal propagation makes such attacks possible in the first place, but at the same time poses a challenge for the attacker: The jamming signal does not only reach the victim device but also other neighboring devices, preventing precise attack targeting.**

**In this work, we solve this challenge by leveraging the emerging reconfigurable intelligent surface (RIS) technology for the first**

signal, preventing a victim receiver from correctly decoding it. Crucially, loss of connectivity impacts the functionality of wireless devices and can thus have potentially far-reaching consequences, such as in smart grids, smart transportation, and healthcare systems. Recent media reports underscore the real-world threat potential of jamming attacks, *e.g.*, criminals disabling smart home security systems [5, 6] and preventing cars from locking [7].

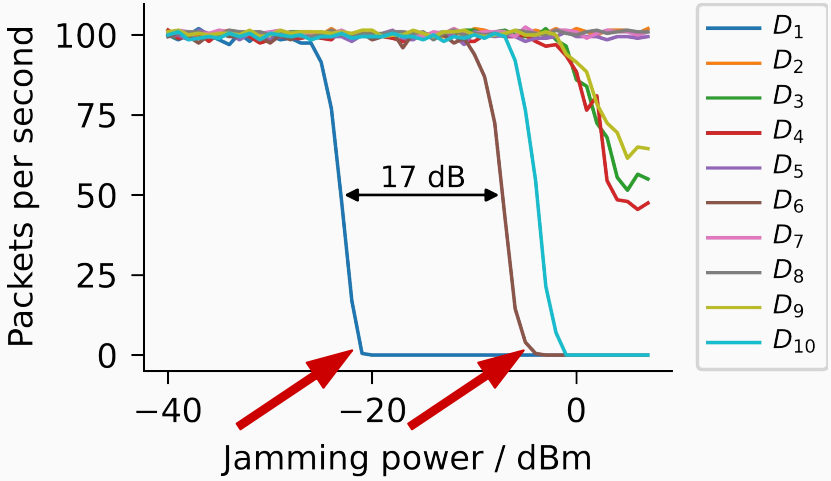
This basic attack principle has previously been studied by

- Environmental variation
- Sub-wavelength settings
- Antenna comparison
- And more!

Contact: philipp.mackensen@rub.de, paul.staat@mpi-sp.org

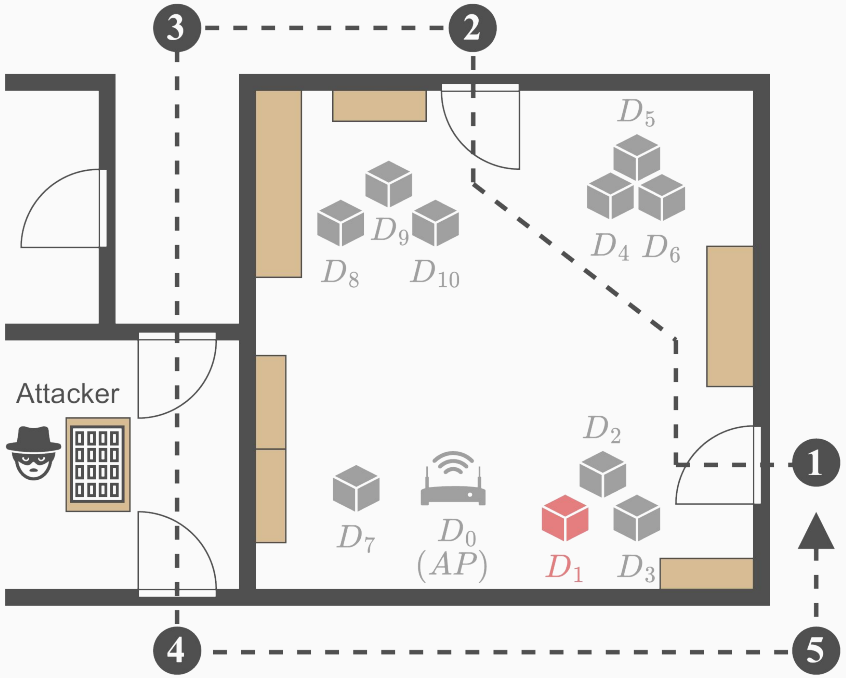
# Effect of Jamming Signal Power

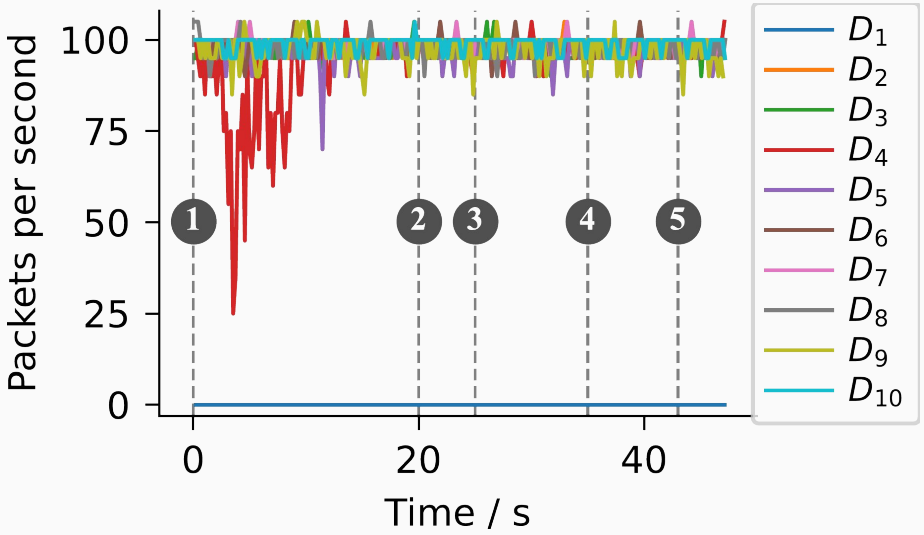
- Attacker can increase power by another 17 dB (linear factor 50) before any other device ($D_6$) is jammed
- RIS-based signal power optimization shapes Jamming-to-Signal Ratios (JSRs)



# Environmental Variation - Human Motion

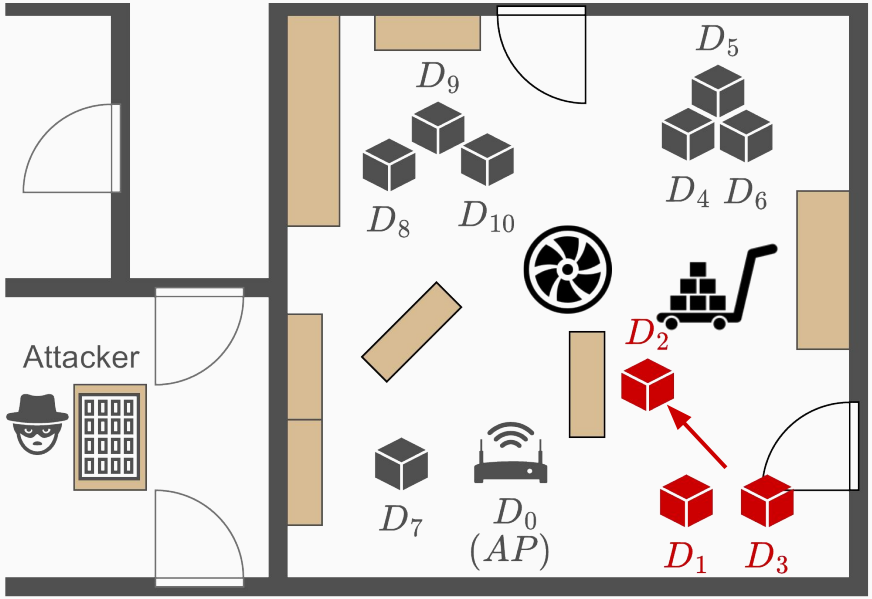
- *How does human motion affect the stability of the RIS configuration?*

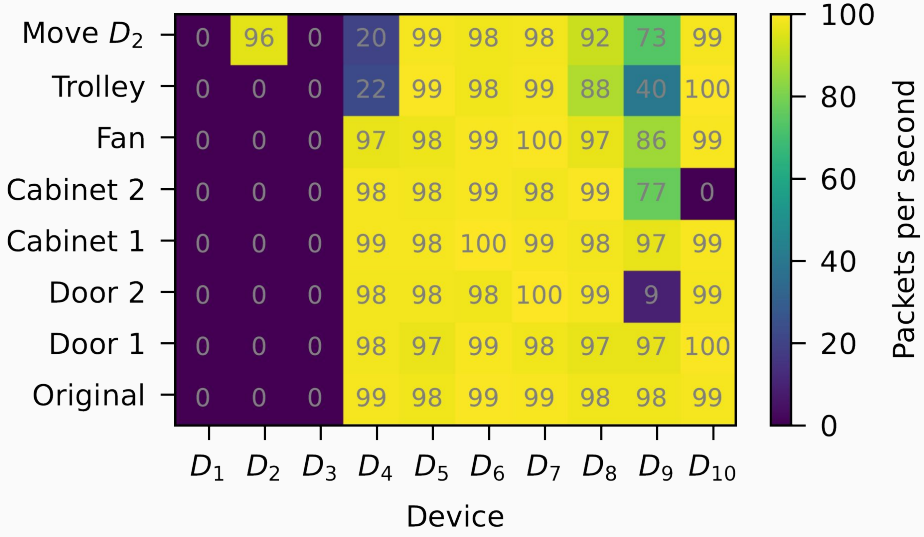


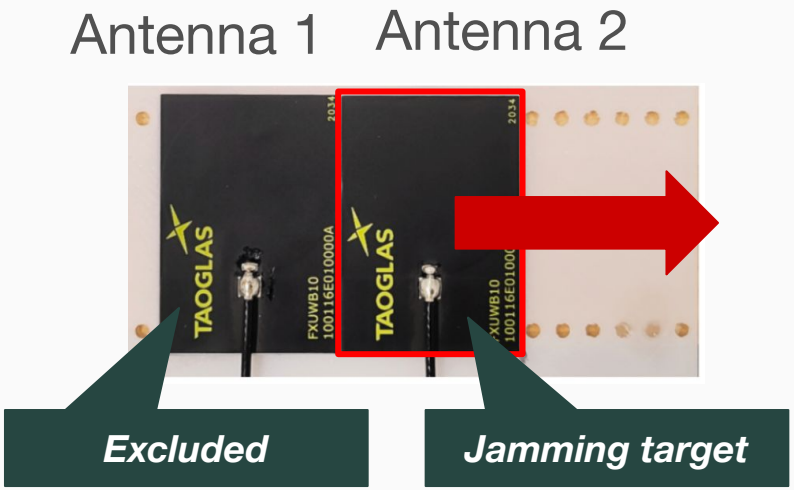
# Environmental Variation - Incremental Changes

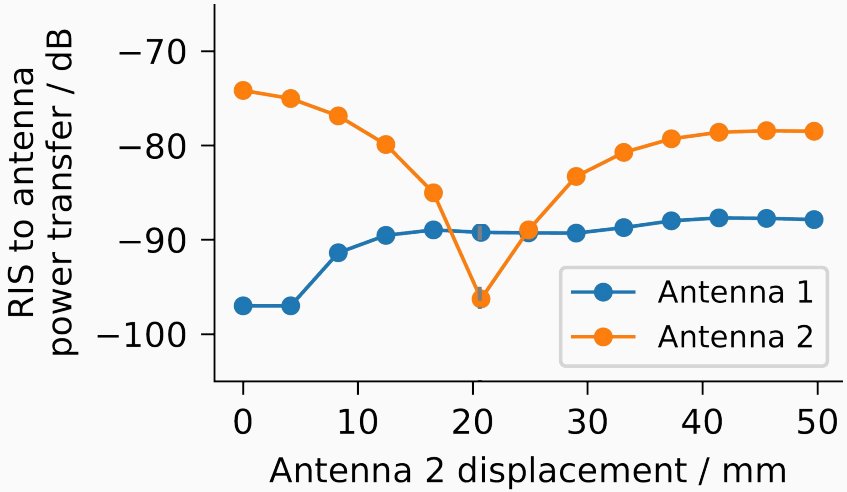
- Targeting cluster consisting of $D_1$, $D_2$ and $D_3$.



# Detailed Look into the Spatial-Domain




- We achieved up to ~30 dB isolation between antennas in extreme proximity
  - Spatial correlation?!
- Enhanced spatial diversity due to mutual antenna coupling
  - Isolation of Antenna 1 reduces as Antenna 2 moves away