MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

YOUR WI-FI IS THE EAVESDROPPER'S RADAR: HOW TO COUNTER PRIVACY THREATS OF WIRELESS SENSING

Paul Staat[1,2]

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

Contact: paul.staat@mpi-sp.org

RuhrSec 2023

May 11, 2023

ABOUT ME

Paul Staat

PhD Student since 2019, supervised by Prof. Christof Paar

Max Planck Institute for Security and Privacy (MPI-SP)

Research interests:

- Radio frequency systems
- Wireless security
- Hardware security

COLLABORATORS


Simon Mulzer


Stefan Roth


Veelasha Moonsamy


Markus Heinrichs


Rainer Kronberger


Aydin Sezgin


Christof Paar

UBIQUITOUS WI-FI

Photos: Noupload, luis2500gx, Muhammad Abdullah, haus_automation, USA-Reiseblogger, luis2500gx at pixabay.com; cottonbro, Fabian Hurnaus, Torsten Dettlaff, Pixabay at pexels.com

UBIQUITOUS WI-FI – PRIVACY THREATS

Application Security

Network-Level Inference

<u>This talk:</u>
Physical-Layer Wireless Sensing

The Cybersecurity 202: Smart home devices with known security flaws are still on the market, researchers say

Peek-a-Boo: I see your smart home activities, even encrypted!

Abbas Acar[1], Hossein Fereidooni[2], Tigist Abera[2], Amit Kumar Sikder[1], Markus Miettinen[2], Hidayet Aksu[1], Mauro Conti[3], Ahmad-Reza Sadeghi[2], Selcuk Uluagac[1]
[1]Florida International University - {aacar001,asikd003,haksu,suluagac}@fiu.edu

Violating Privacy Through Walls by Passive Monitoring of Radio Windows

Arijit Banerjee
University of Utah
Salt Lake City, UT, USA
arijit@cs.utah.edu

Dustin Maas
Xandem Technology
Salt Lake City, UT, USA
dustin@xandem.com

Maurizio Bocca
Politecnico di Milano
Milano, Italy
maurizio.bocca@polimi.it

Neal Patwari
University of Utah & Xandem Technology
Salt Lake City, UT, USA
npatwari@ece.utah.edu

Sneha Kasera
University of Utah
Salt Lake City, UT, USA
kasera@cs.utah.edu

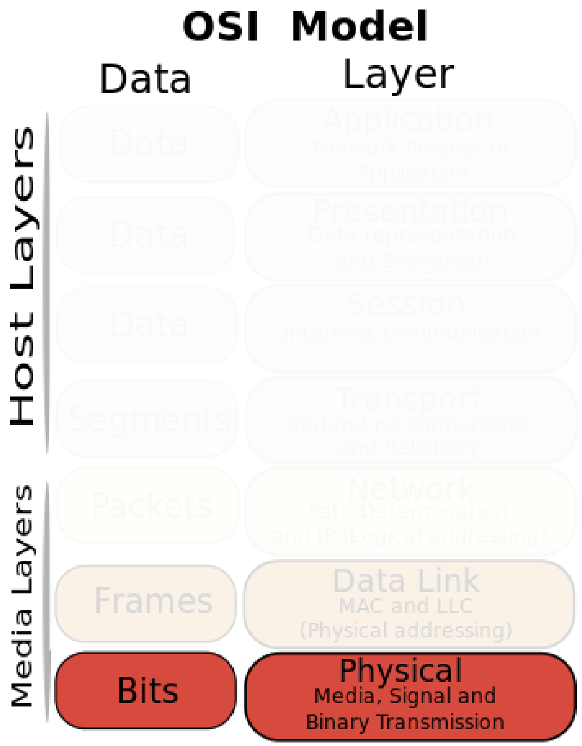
TALK OVERVIEW

1. The Wi-Fi physical layer

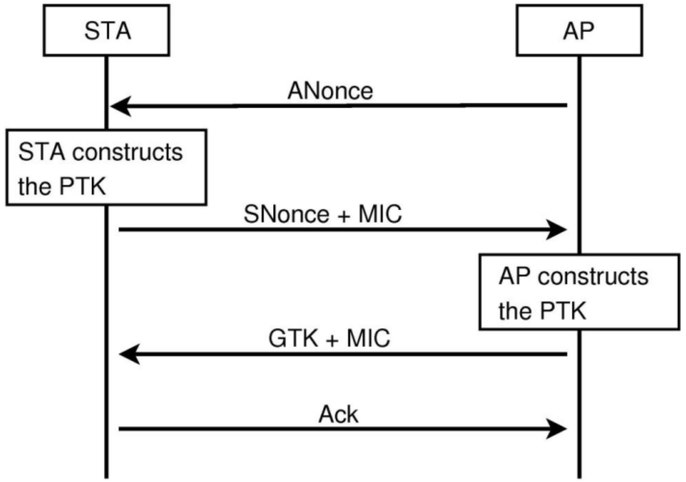
2. Wireless sensing and privacy implications

3. IRShield: Countermeasure against adversarial wireless sensing

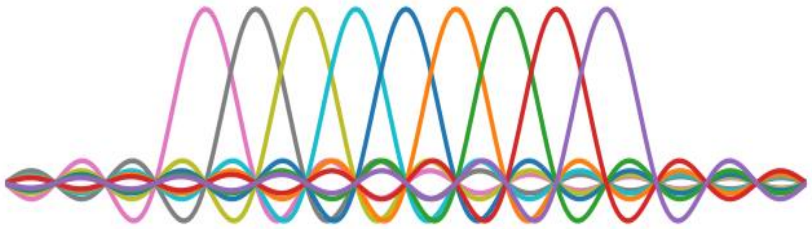
IEEE 802.11 WI-FI



Source: wikimedia.org



This talk :)

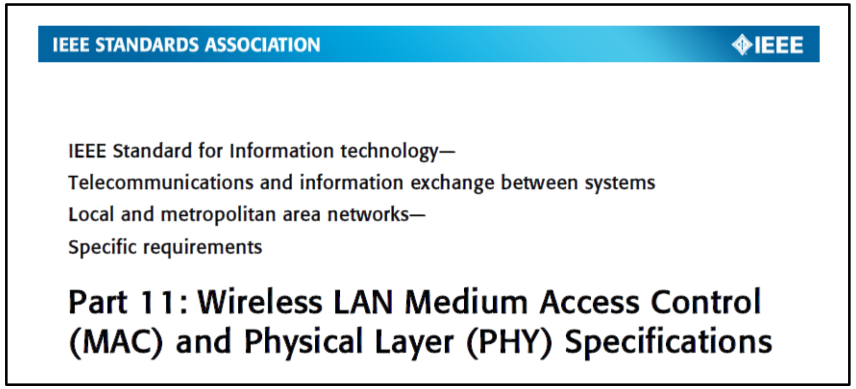


WI-FI ON THE PHYSICAL LAYER

Each Wi-Fi packet (PPDU) begins with a preamble

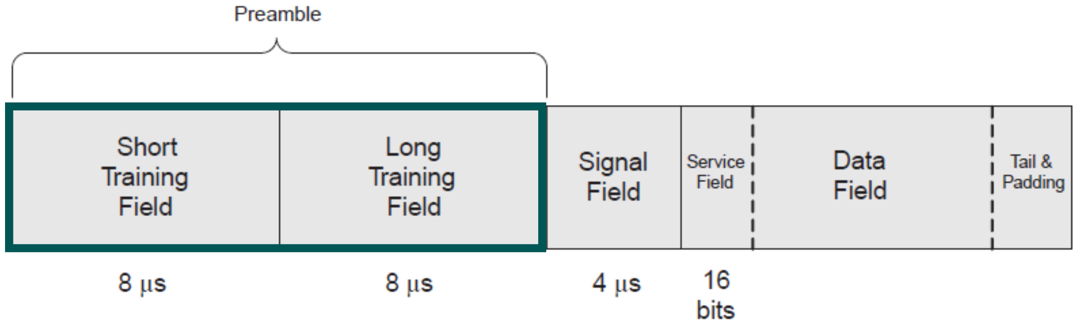
- Signal detection
- Frequency estimation
- **<u>Channel estimation</u>**

Preamble:
Known sequence, unencrypted


IEEE STANDARDS ASSOCIATION IEEE

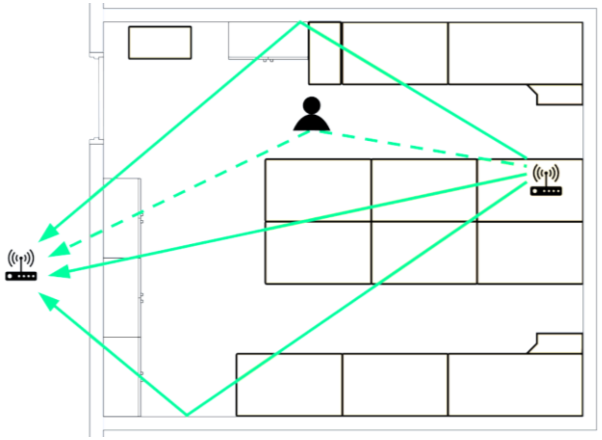
IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications



Perahia and Stacey, „Next Generation Wireless LANs“, Cambridge University Press, 2008

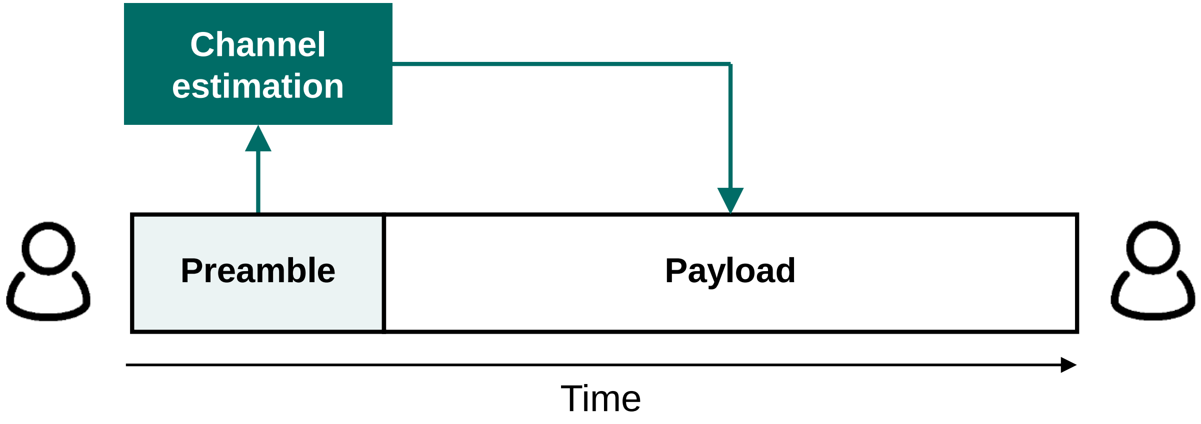
WI-FI CHANNEL ESTIMATION



Radio signal propagation distorts transmitted signal

- Attenuation, reflection, scattering, ...

Channel effects must be removed to receive the payload data



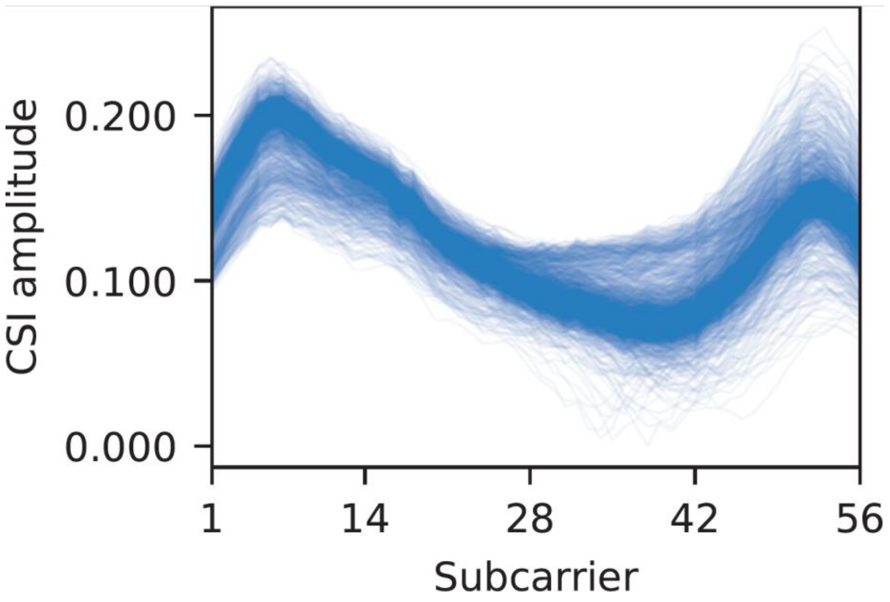
Every Wi-Fi receiver estimates the radio channel

WI-FI CHANNEL ESTIMATION II

Channel State Information (CSI)

Received signal strength indication (RSSI) „on steroids“

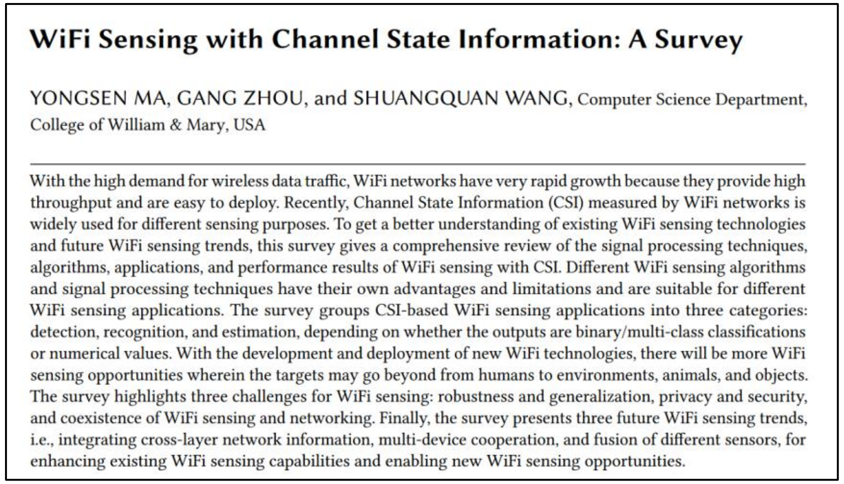
Complex-valued frequency-domain transfer function of the wireless channel



WIRELESS SENSING

Extract information about the surrounding environment from the wireless channel

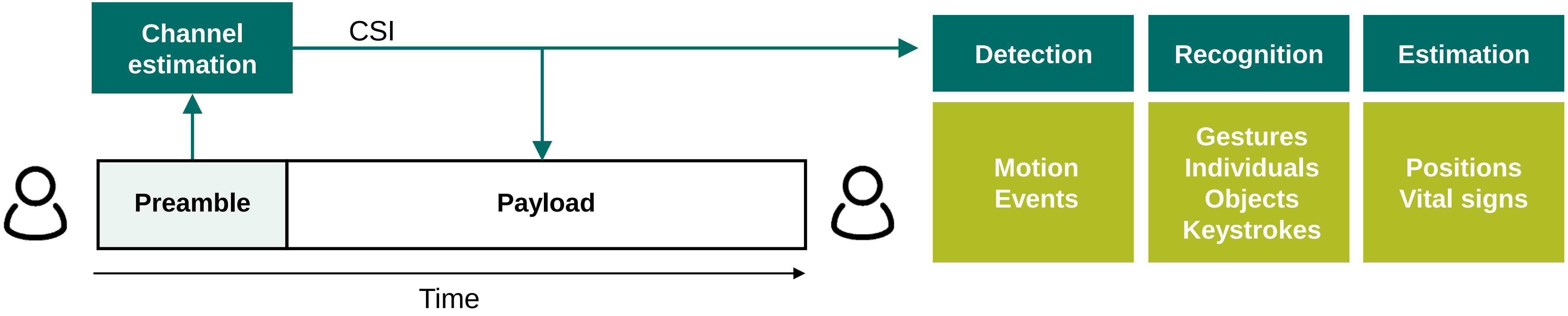
Wireless channel depends on environment


WiFi Sensing with Channel State Information: A Survey

YONGSEN MA, GANG ZHOU, and SHUANGQUAN WANG, Computer Science Department, College of William & Mary, USA

With the high demand for wireless data traffic, WiFi networks have very rapid growth because they provide high throughput and are easy to deploy. Recently, Channel State Information (CSI) measured by WiFi networks is widely used for different sensing purposes. To get a better understanding of existing WiFi sensing technologies and future WiFi sensing trends, this survey gives a comprehensive review of the signal processing techniques, algorithms, applications, and performance results of WiFi sensing with CSI. Different WiFi sensing algorithms and signal processing techniques have their own advantages and limitations and are suitable for different WiFi sensing applications. The survey groups CSI-based WiFi sensing applications into three categories: detection, recognition, and estimation, depending on whether the outputs are binary/multi-class classifications or numerical values. With the development and deployment of new WiFi technologies, there will be more WiFi sensing opportunities wherein the targets may go beyond from humans to environments, animals, and objects. The survey highlights three challenges for WiFi sensing: robustness and generalization, privacy and security, and coexistence of WiFi sensing and networking. Finally, the survey presents three future WiFi sensing trends, i.e., integrating cross-layer network information, multi-device cooperation, and fusion of different sensors, for enhancing existing WiFi sensing capabilities and enabling new WiFi sensing opportunities.

Ma et al., “WiFi Sensing with Channel State Information: A Survey“. ACM Comput. Surv., vol. 52, no. 3, 2019.



COMING TO A WIRELESS NETWORK NEAR YOU

Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond

Fan Liu, *Member, IEEE*, Yuanhao Cui, *Member, IEEE*, Christos Masouros, *Senior Member, IEEE*, Jie Xu, *Member, IEEE*, Tony Xiao Han, *Senior Member, IEEE*, Yonina C. Eldar, *Fellow, IEEE*, and Stefano Buzzi, *Senior Member, IEEE*

***Abstract*—As the standardization of 5G solidifies, researchers are speculating what 6G will be. The integration of sensing functionality is emerging as a key feature of the 6G Radio theoretical limits to physical layer performance tradeoffs, and the cross-layer design tradeoffs. Next, we discuss the signal processing aspects of ISAC, namely ISAC waveform design and**

An Overview on IEEE 802.11bf: WLAN Sensing

Rui Du*, *Member, IEEE*, Hailiang Xie*, *Graduate Student Member, IEEE*, Mengshi Hu, Narengerile, Yan Xin, Stephen McCann, *Senior Member, IEEE*, Michael Montemurro, Tony Xiao Han, *Senior Member, IEEE*, and Jie Xu, *Senior Member, IEEE*

***Abstract*—With recent advancements, the wireless local area network (WLAN) or wireless fidelity (Wi-Fi) technology has been successfully utilized to realize sensing functionalities such as detection, localization, and recognition. However, the WLANs standards are developed mainly for the purpose of communica-**

sensing, also known as *Wi-Fi sensing*[1], has recently attracted growing interests from both academia and industry.

WLAN sensing is a technology that uses Wi-Fi signals to perform sensing tasks, by exploiting prevalent Wi-Fi in-

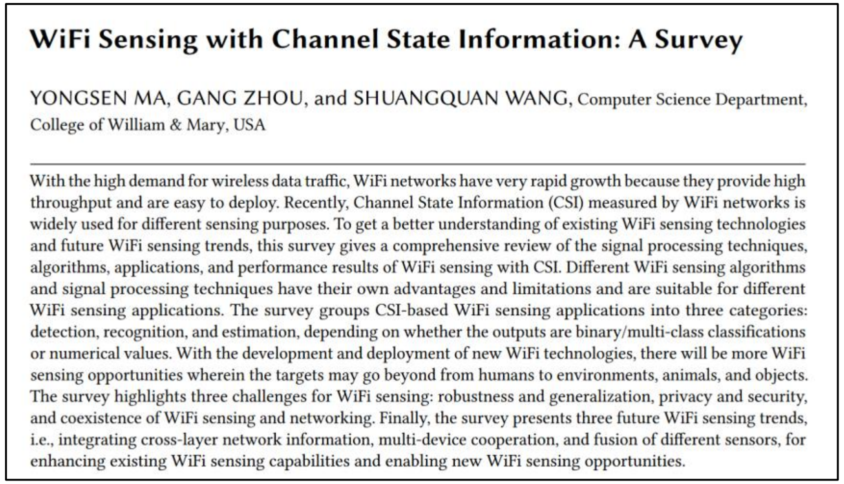
Channel Sounding

***Bluetooth*® Change Request**

- **Revision:** r02
- **Revision Date:** 2022-11-18
- **Prepared By:** Core Specification Working Group
- **Feedback Email:** core-main@bluetooth.org

ADVERSARIAL WIRELESS SENSING

Extract information about the surrounding environment from the wireless channel

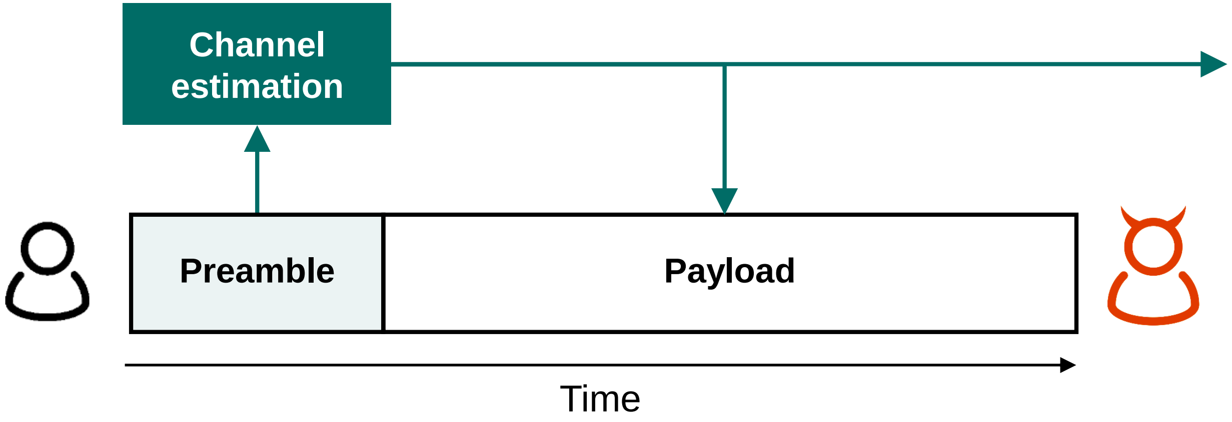


WiFi Sensing with Channel State Information: A Survey

YONGSEN MA, GANG ZHOU, and SHUANGQUAN WANG, Computer Science Department, College of William & Mary, USA

With the high demand for wireless data traffic, WiFi networks have very rapid growth because they provide high throughput and are easy to deploy. Recently, Channel State Information (CSI) measured by WiFi networks is widely used for different sensing purposes. To get a better understanding of existing WiFi sensing technologies and future WiFi sensing trends, this survey gives a comprehensive review of the signal processing techniques, algorithms, applications, and performance results of WiFi sensing with CSI. Different WiFi sensing algorithms and signal processing techniques have their own advantages and limitations and are suitable for different WiFi sensing applications. The survey groups CSI-based WiFi sensing applications into three categories: detection, recognition, and estimation, depending on whether the outputs are binary/multi-class classifications or numerical values. With the development and deployment of new WiFi technologies, there will be more WiFi sensing opportunities wherein the targets may go beyond from humans to environments, animals, and objects. The survey highlights three challenges for WiFi sensing: robustness and generalization, privacy and security, and coexistence of WiFi sensing and networking. Finally, the survey presents three future WiFi sensing trends, i.e., integrating cross-layer network information, multi-device cooperation, and fusion of different sensors, for enhancing existing WiFi sensing capabilities and enabling new WiFi sensing opportunities.

Ma et al., “WiFi Sensing with Channel State Information: A Survey“. ACM Comput. Surv., vol. 52, no. 3, 2019.



Detection | **Recognition** | **Estimation**

Privacy violation by rogue receiver

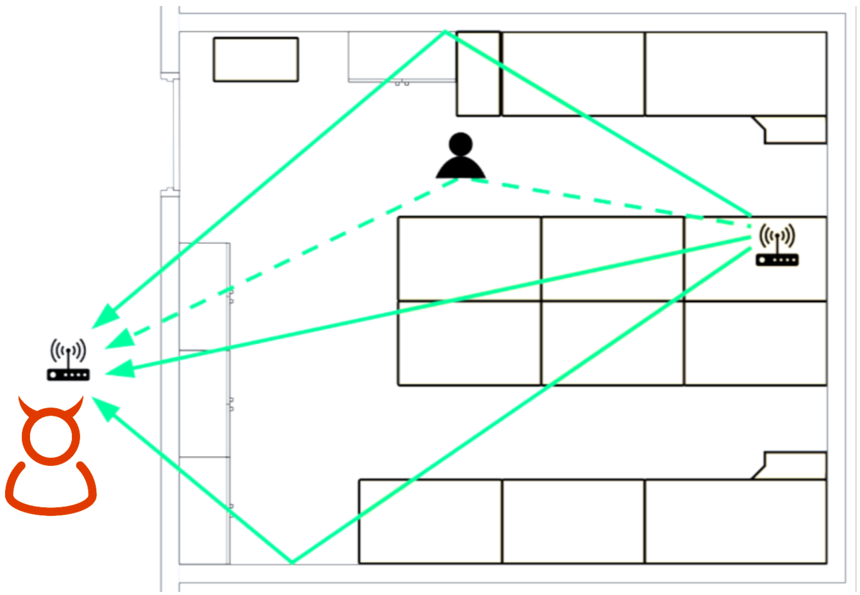
PRIVACY IMPLICATIONS

Unwanted channel (= radio wave propagation) towards passive eavesdropper

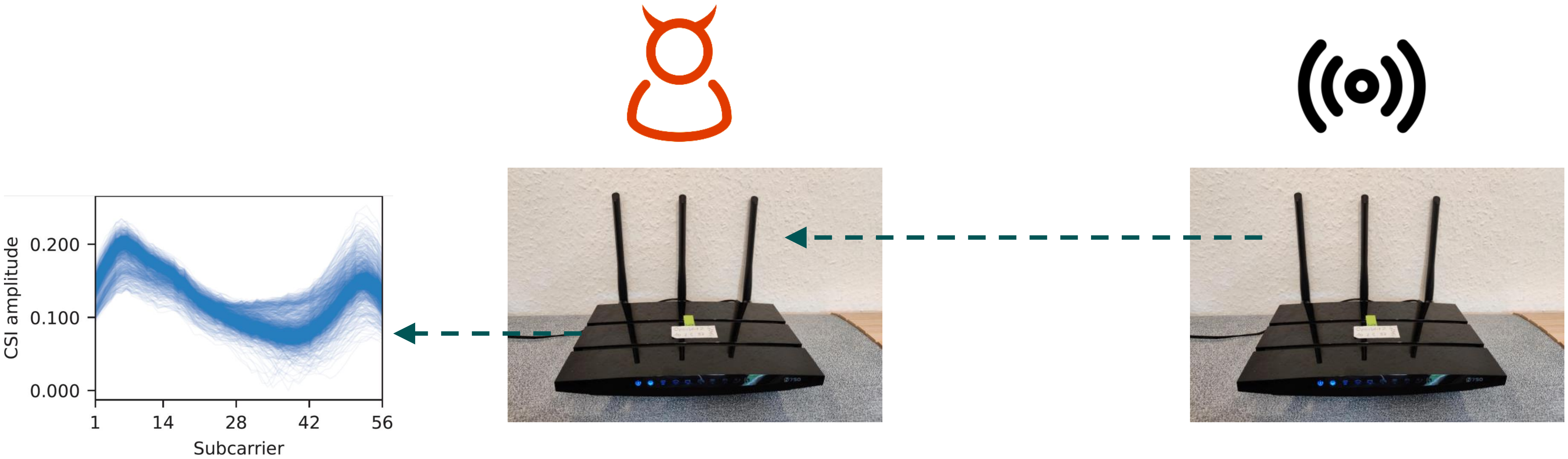
Remote monitoring: Obtain sensitive information from the inside of the environment

Potentially same capabilities as legitimate parties

Detection	Recognition	Estimation
Motion Events	Gestures Individuals Objects Keystrokes	Positions Vital signs



STATE-OF-THE-ART: ADVERSARIAL MOTION DETECTION

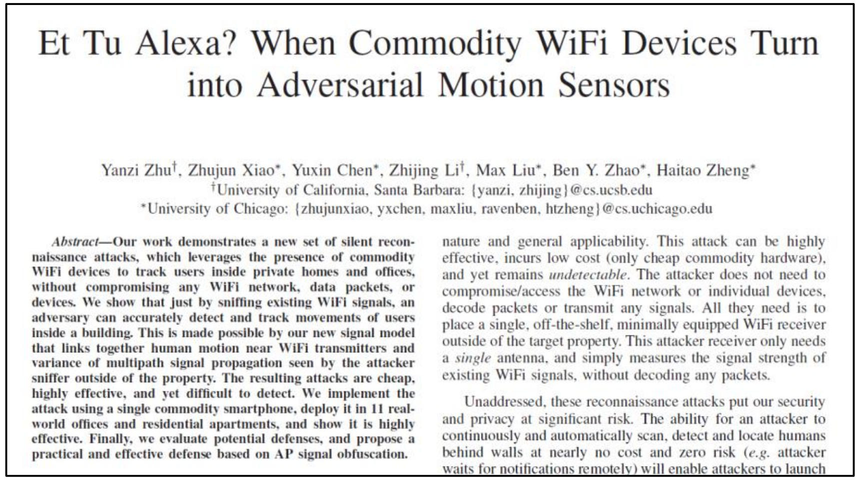


CSI

TP-Link N750 router, receiver

TP-Link N750 router, transmitter

STATE-OF-THE-ART: ADVERSARIAL MOTION DETECTION



Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors

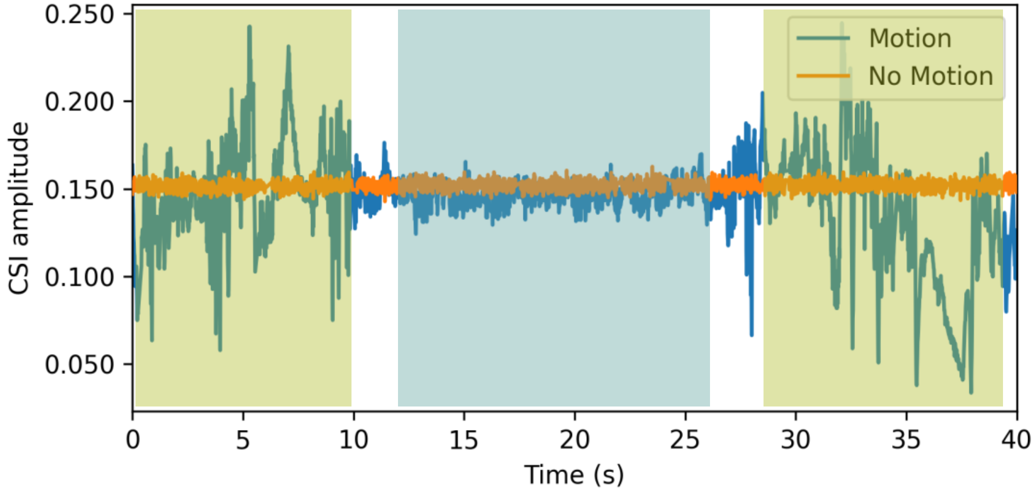
Yanzi Zhu†, Zhujun Xiao*, Yuxin Chen*, Zhijing Li†, Max Liu*, Ben Y. Zhao*, Haitao Zheng*
†University of California, Santa Barbara: {yanzi, zhijing}@cs.ucsb.edu
*University of Chicago: {zhujunxiao, yxchen, maxliu, ravenben, htzheng}@cs.uchicago.edu

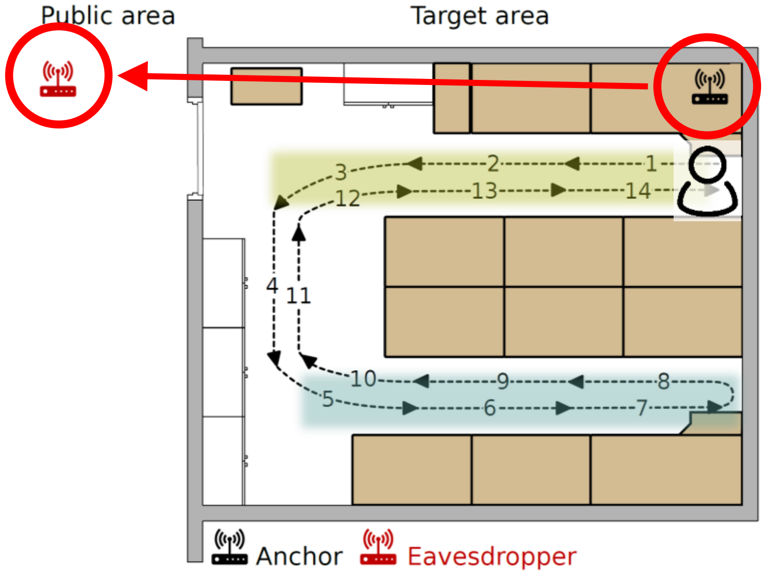
***Abstract*—Our work demonstrates a new set of silent reconnaissance attacks, which leverages the presence of commodity WiFi devices to track users inside private homes and offices, without compromising any WiFi network, data packets, or devices. We show that just by sniffing existing WiFi signals, an adversary can accurately detect and track movements of users inside a building. This is made possible by our new signal model that links together human motion near WiFi transmitters and variance of multipath signal propagation seen by the attacker sniffer outside of the property. The resulting attacks are cheap, highly effective, and yet difficult to detect. We implement the attack using a single commodity smartphone, deploy it in 11 real-world offices and residential apartments, and show it is highly effective. Finally, we evaluate potential defenses, and propose a practical and effective defense based on AP signal obfuscation.**

nature and general applicability. This attack can be highly effective, incurs low cost (only cheap commodity hardware), and yet remains *undetectable*. The attacker does not need to compromise/access the WiFi network or individual devices, decode packets or transmit any signals. All they need is to place a single, off-the-shelf, minimally equipped WiFi receiver outside of the target property. This attacker receiver only needs a *single* antenna, and simply measures the signal strength of existing WiFi signals, without decoding any packets.

Unaddressed, these reconnaissance attacks put our security and privacy at significant risk. The ability for an attacker to continuously and automatically scan, detect and locate humans behind walls at nearly no cost and zero risk (*e.g.* attacker waits for notifications remotely) will enable attackers to launch

Zhu et al., "Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors," in 27th Annual Network and Distributed System Security Symposium, NDSS 2020.





Signal variation reveals human motion!

STATE-OF-THE-ART: ADVERSARIAL MOTION DETECTION

Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors

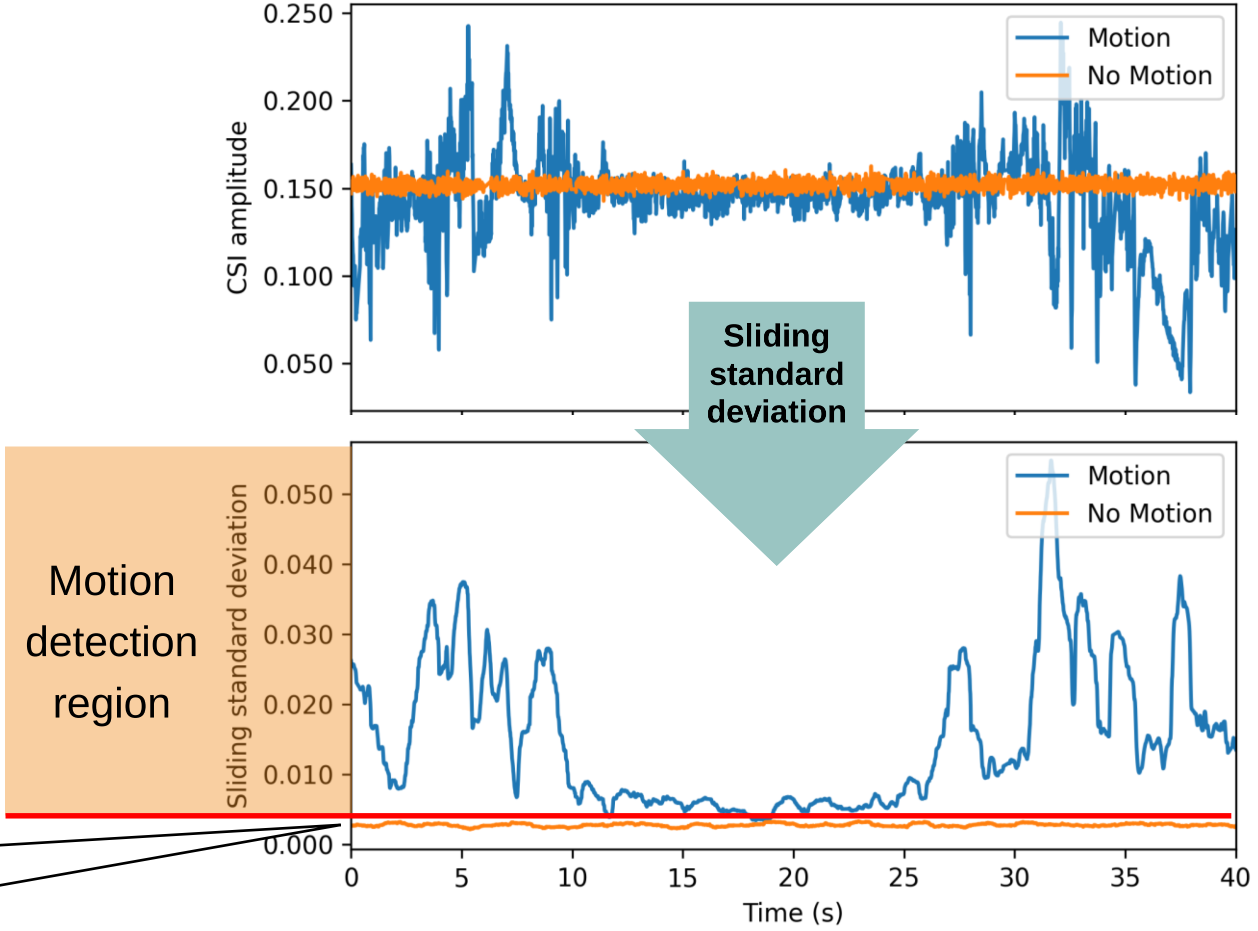
Yanzi Zhu[†], Zhujun Xiao[*], Yuxin Chen[*], Zhijing Li[†], Max Liu[*], Ben Y. Zhao[*], Haitao Zheng[*]
[†]University of California, Santa Barbara: {yanzi, zhijing}@cs.ucsb.edu
[*]University of Chicago: {zhujunxiao, yxchen, maxliu, ravenben, htzheng}@cs.uchicago.edu

Abstract—Our work demonstrates a new set of silent reconnaissance attacks, which leverages the presence of commodity WiFi devices to track users inside private homes and offices, without compromising any WiFi network, data packets, or devices. We show that just by sniffing existing WiFi signals, an adversary can accurately detect and track movements of users inside a building. This is made possible by our new signal model that links together human motion near WiFi transmitters and variance of multipath signal propagation seen by the attacker sniffer outside of the property. The resulting attacks are cheap, highly effective, and yet difficult to detect. We implement the attack using a single commodity smartphone, deploy it in 11 real-world offices and residential apartments, and show it is highly effective. Finally, we evaluate potential defenses, and propose a practical and effective defense based on AP signal obfuscation.

nature and general applicability. This attack can be highly effective, incurs low cost (only cheap commodity hardware), and yet remains *undetectable*. The attacker does not need to compromise/access the WiFi network or individual devices, decode packets or transmit any signals. All they need is to place a single, off-the-shelf, minimally equipped WiFi receiver outside of the target property. This attacker receiver only needs a *single* antenna, and simply measures the signal strength of existing WiFi signals, without decoding any packets.

Unaddressed, these reconnaissance attacks put our security and privacy at significant risk. The ability for an attacker to continuously and automatically scan, detect and locate humans behind walls at nearly no cost and zero risk (*e.g.* attacker waits for notifications remotely) will enable attackers to launch

Zhu et al., “Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors,” in 27th Annual Network and Distributed System Security Symposium, NDSS 2020.



Adversary derives detection threshold from measurement without motion.

COUNTERMEASURES?

Conflicting goals: Enabling wireless communication vs. preventing wireless sensing

Previous countermeasures:

- Require full-duplex radio or mechanic movement
- Make changes to transmitter and receiver devices
- Affect the wireless quality-of-service

IRSHIELD: A COUNTERMEASURE AGAINST ADVERSARIAL PHYSICAL-LAYER WIRELESS SENSING

Presented at S&P ’22

Joint work with
Simon Mulzer[2], Stefan Roth[2], Veelasha Moonsamy[2], Markus Heinrichs[3], Rainer Kronberger[3], Aydin Sezgin[2]

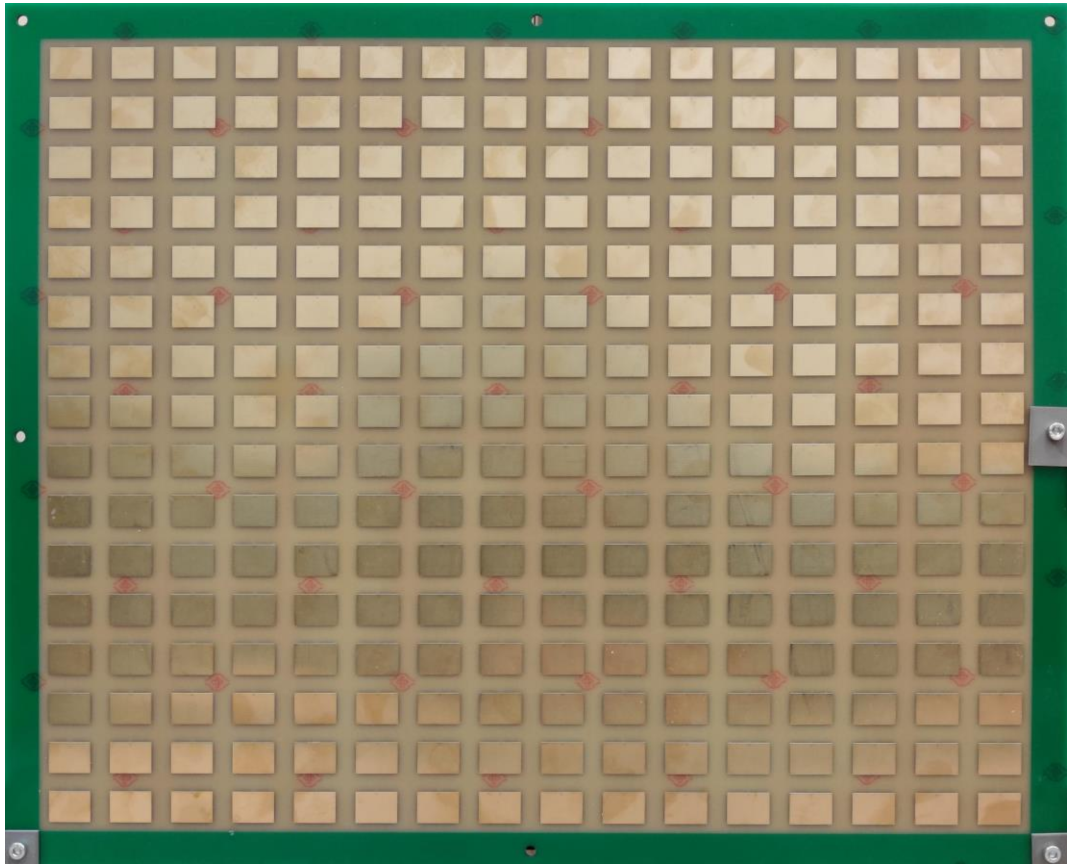
[2] Ruhr University Bochum
[3] TH Köln – University of Applied Sciences

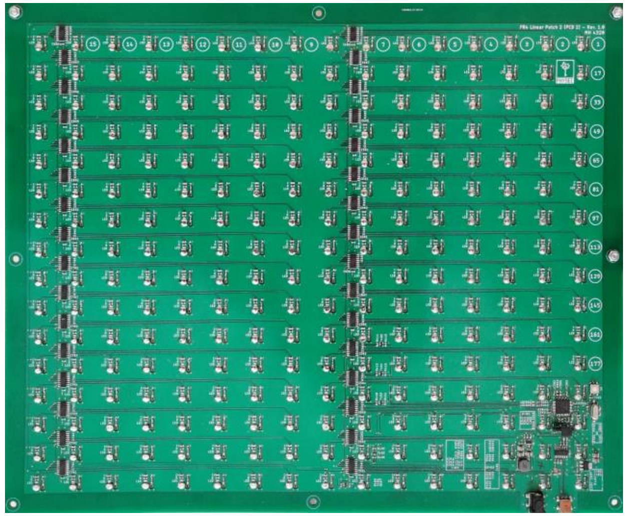
MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

RUB

Technology Arts Sciences TH Köln

INTELLIGENT REFLECTING SURFACE (IRS)

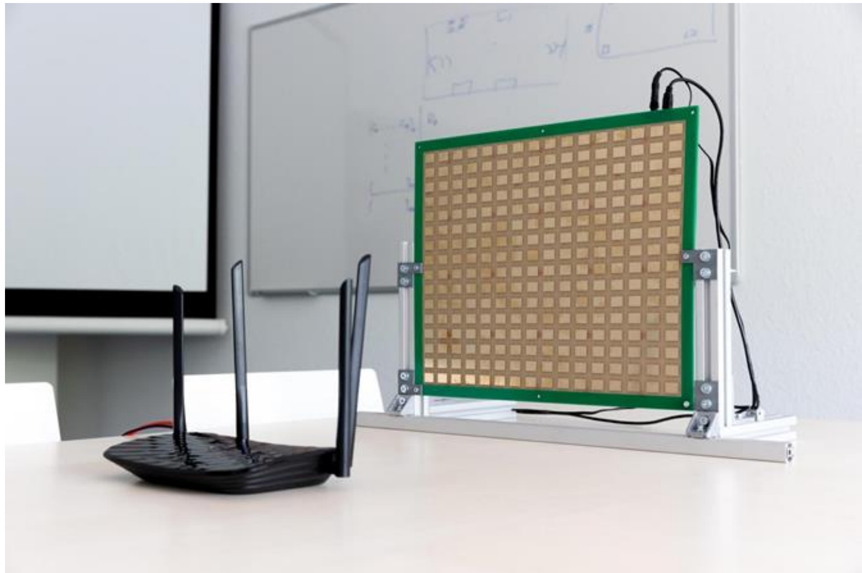




Smart radio propagation environments

IRSHIELD: RESOLVED CHALLENGES

1. Standalone operation, device-agnostic
2. Large IRS configuration space
3. Leaving the wireless quality-of-service unaffected



© Michael Schwettmann, RUB

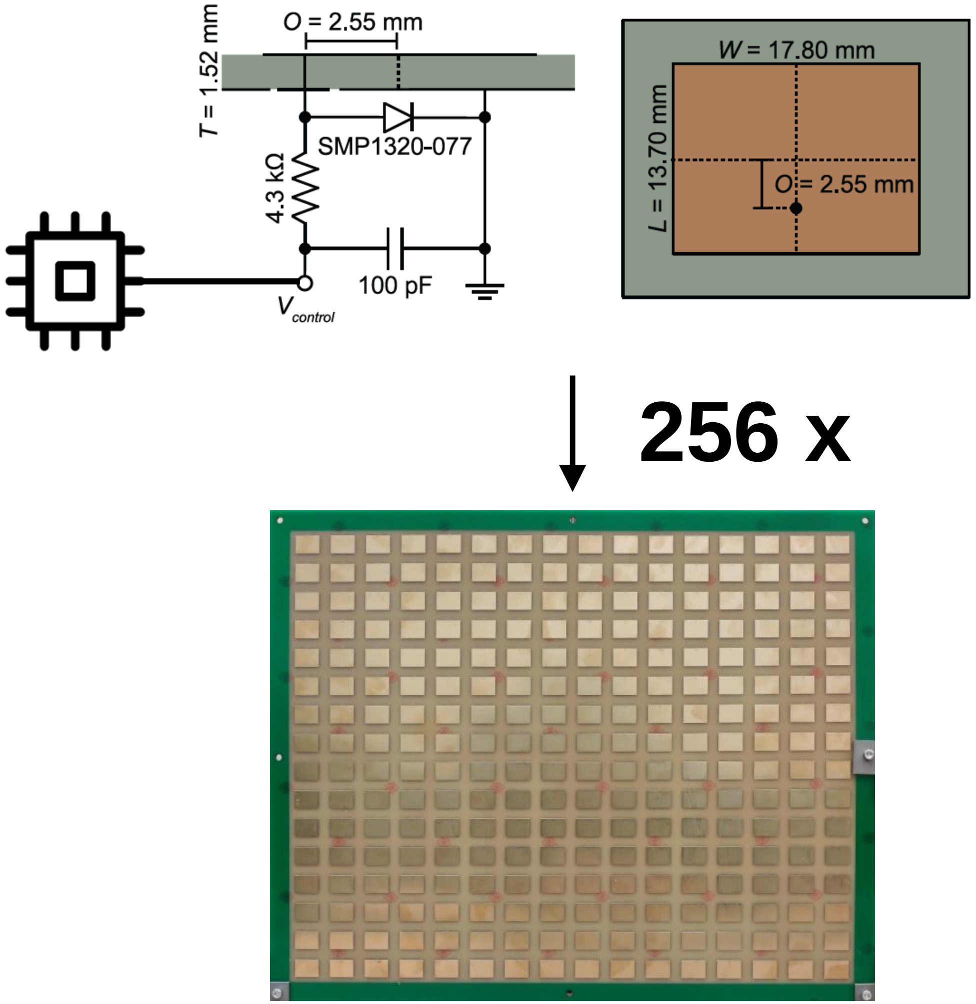
PROTOTYPE IRS DETAILS

Unit cell reflector

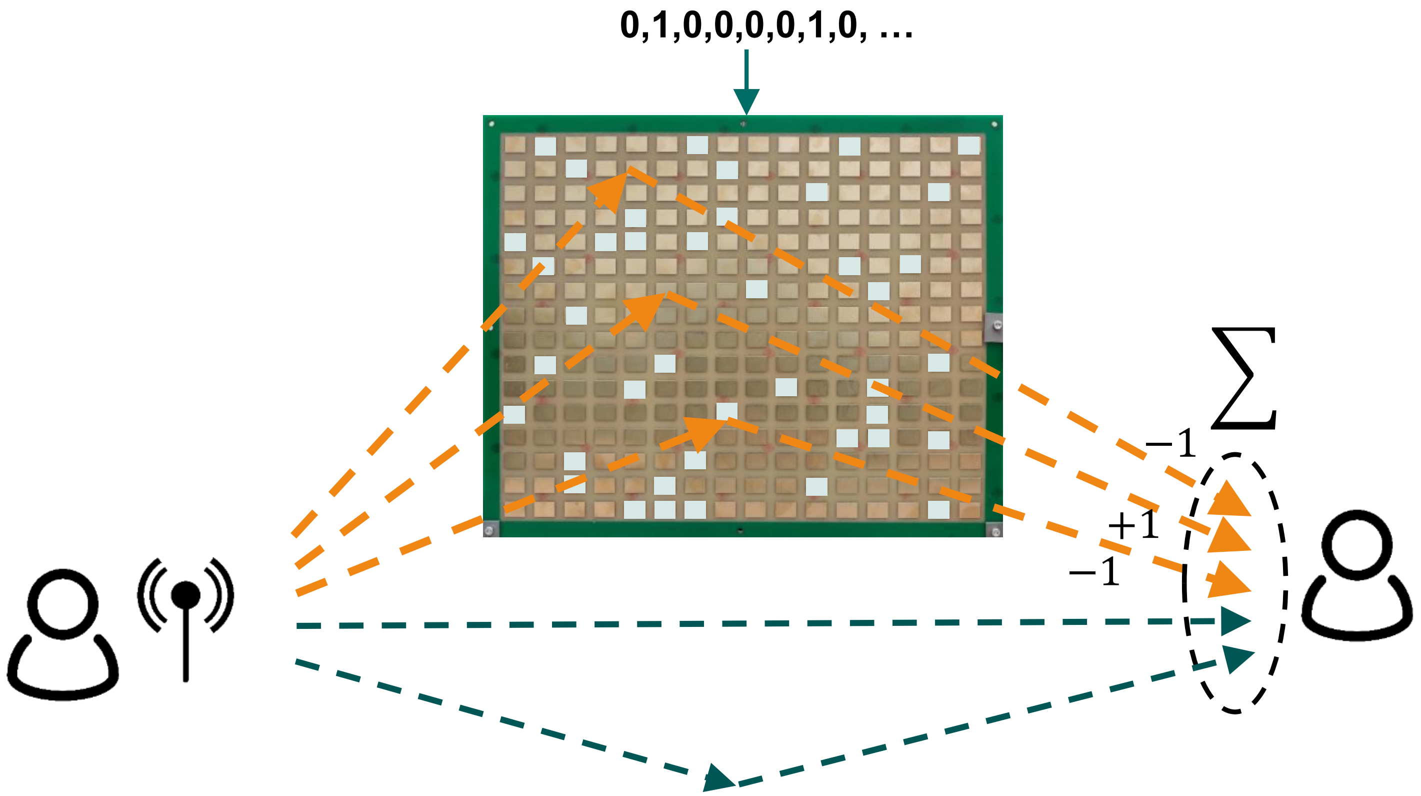
- Multiply reflected wave either by +1 or −1
- PIN diode-based switching
- Digitally configured from a microcontroller

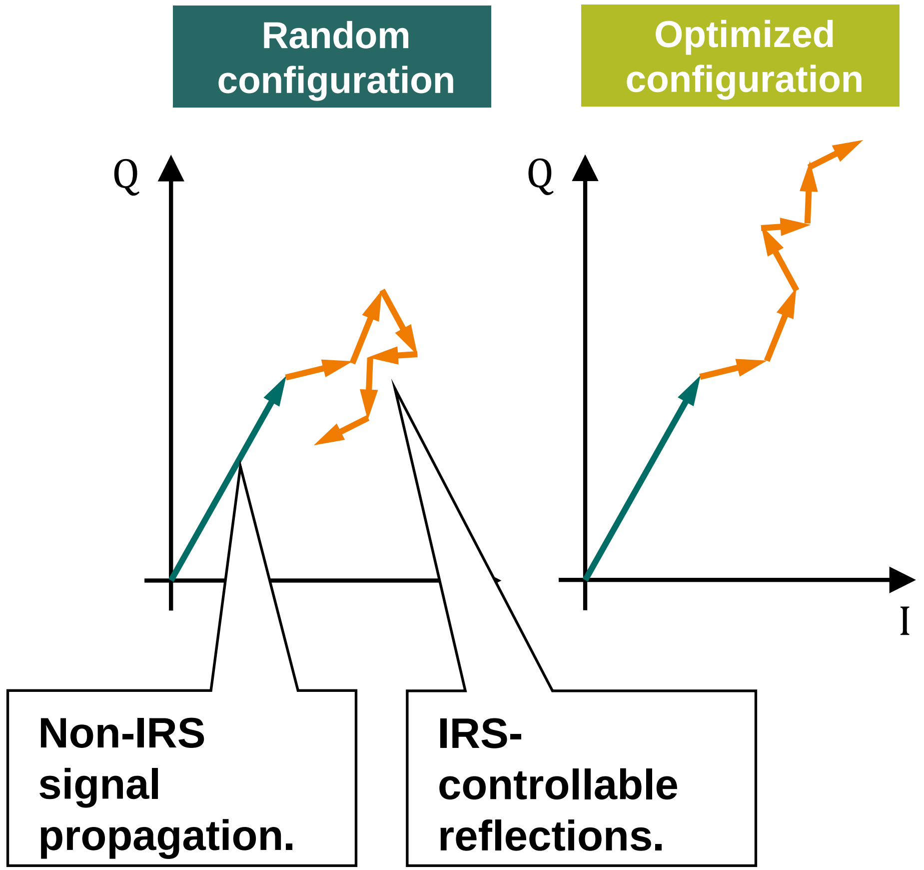
Prototype IRS

- Low-cost printed circuit board (PCB)
- 256 elements
- Operates at 5.35 GHz

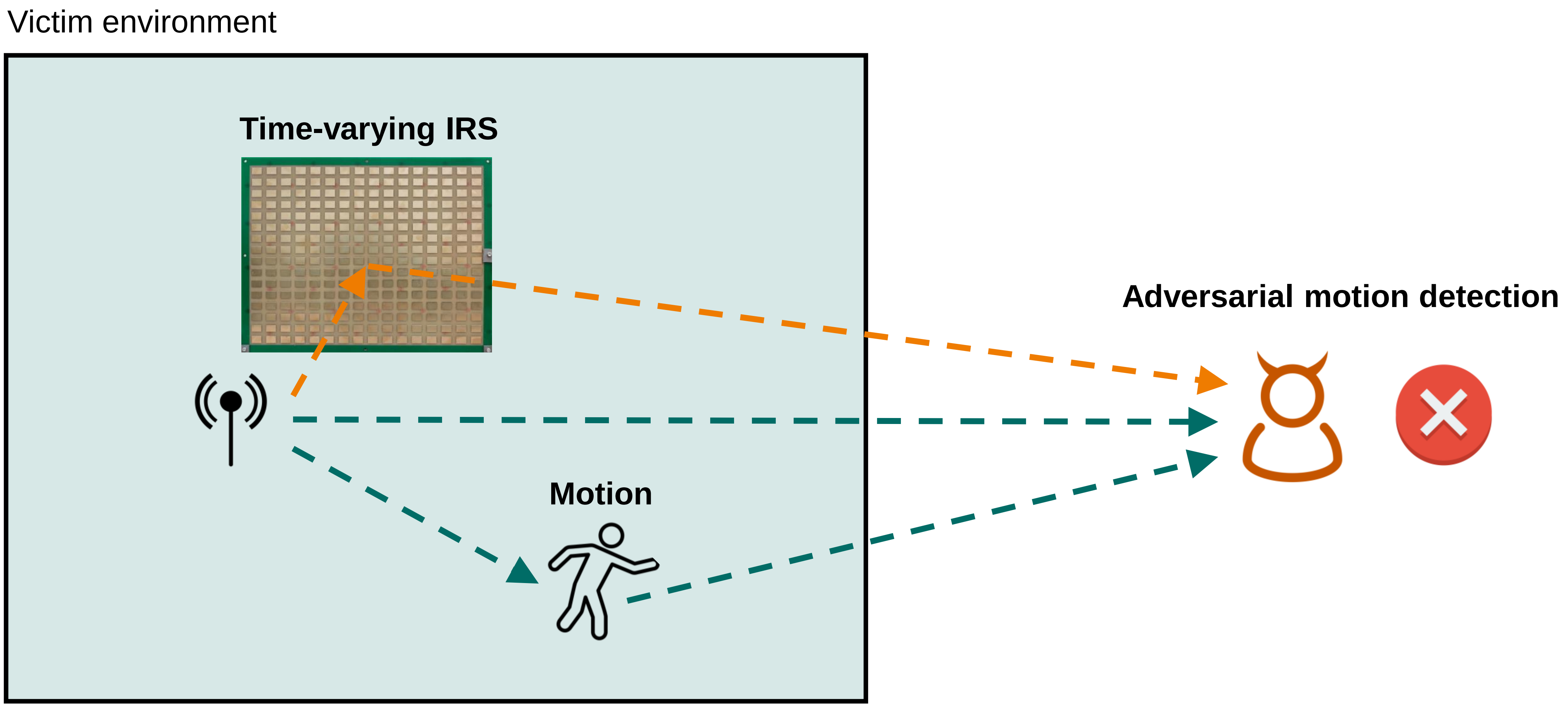


IRS OPERATION PRINCIPLE





IRSHIELD SYSTEM MODEL



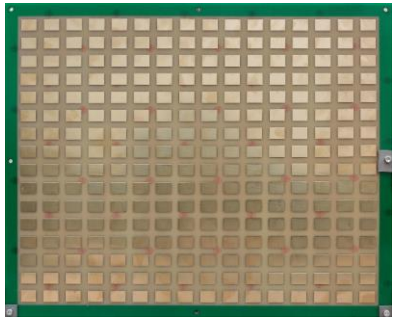
INTUITION OF IRSHIELD

Signal variation

Adversarial motion detection

True positives, true negatives

Time-varying IRS



Signal variation

Adversarial motion detection

False positives, false negatives

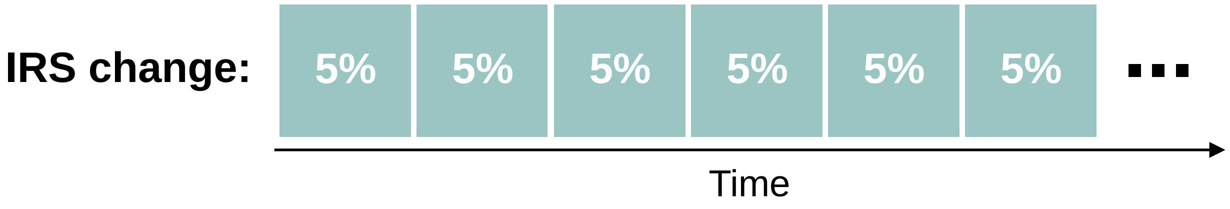
IRS-BASED SIGNAL VARIATION

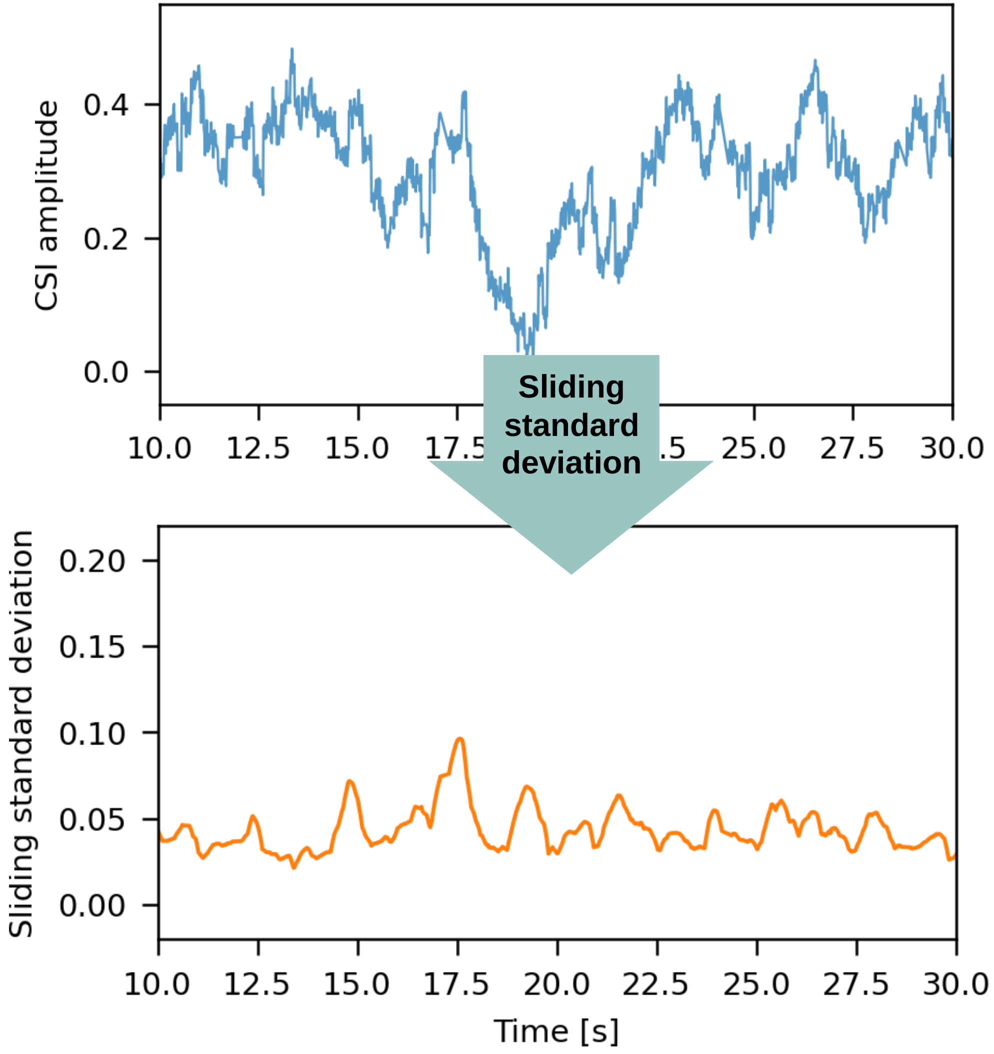
How to produce signal variation with the IRS?

Randomly select 5% out of all IRS elements

➔ Flip their state

➔ Repeat 20 times / second





IRS-BASED SIGNAL VARIATION CONT‘D

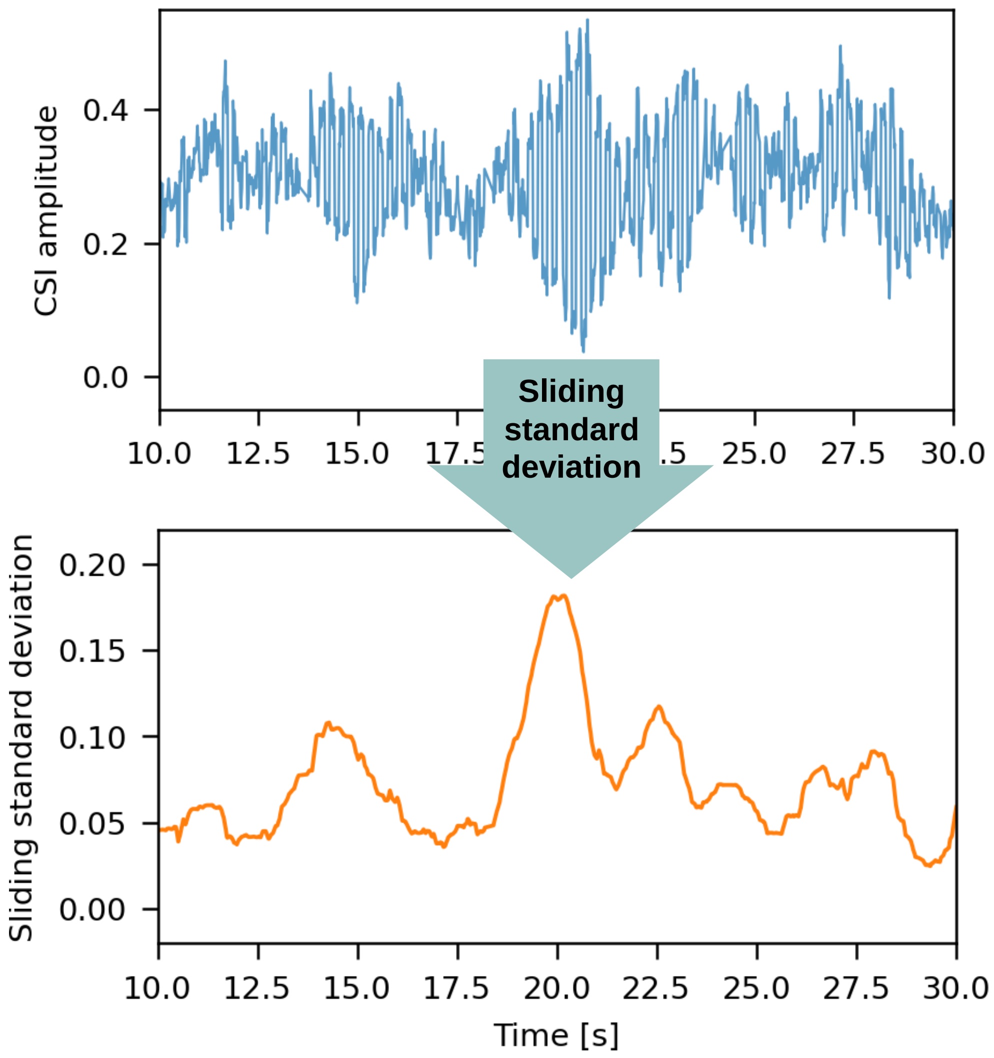
How to vary the sliding standard deviation?

Additionally invert all IRS elements

➔ Interleaved with gradual randomized IRS changes

➔ Larger signal variation range

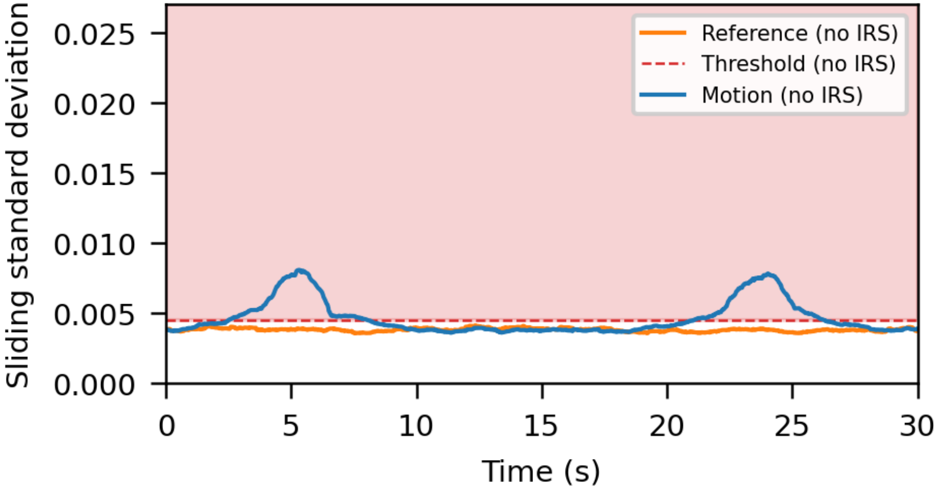
IRS change:

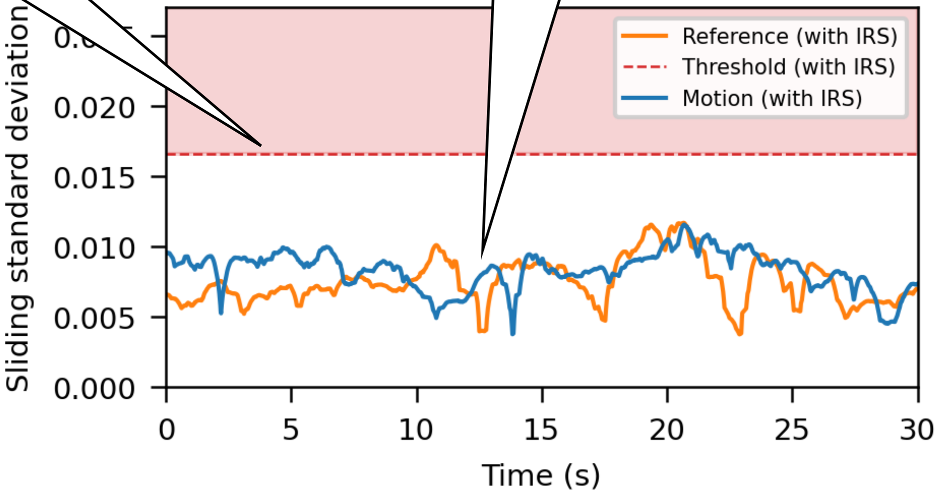


EFFECT OF IRSHIELD

IRShield interferes with threshold finding

No longer distinguishable





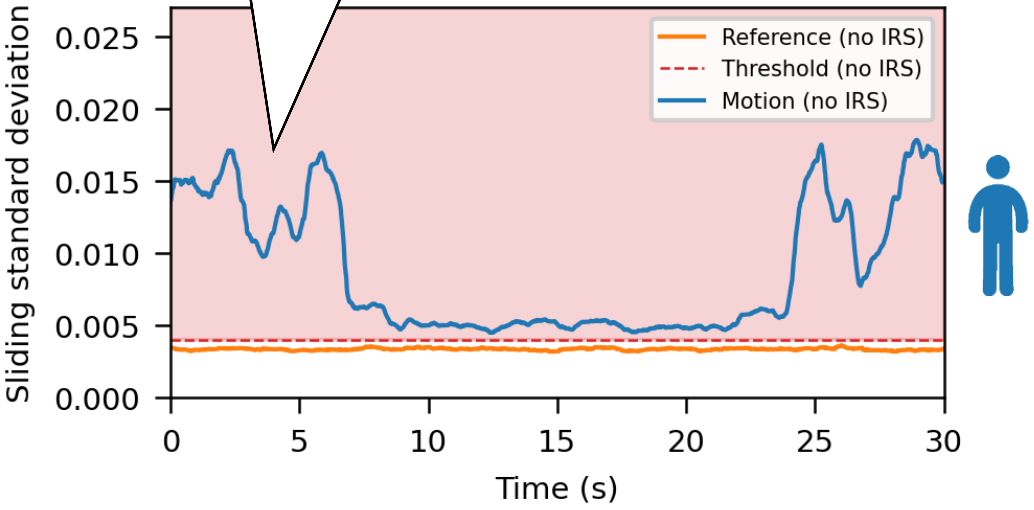
Without IRS

With IRS

EFFECT OF IRSHIELD

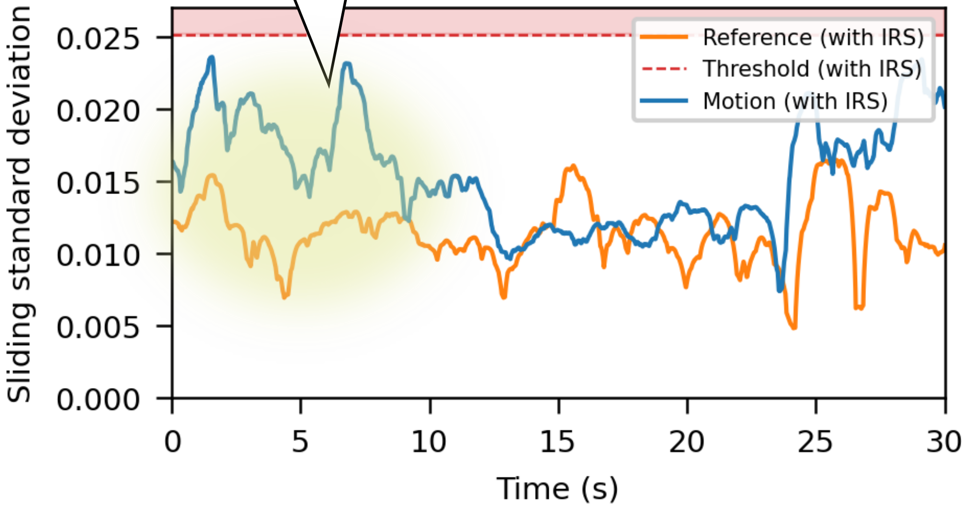
Different transmitter location in target environment

Strong effect of motion within line-of-sight



Without IRS

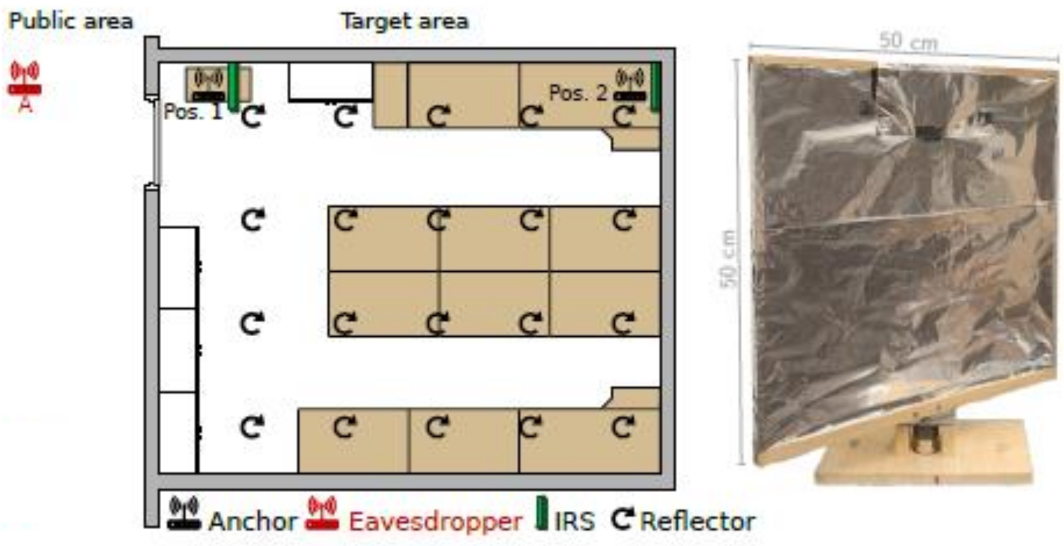
Residual detectability of adaptive attacker



With IRS

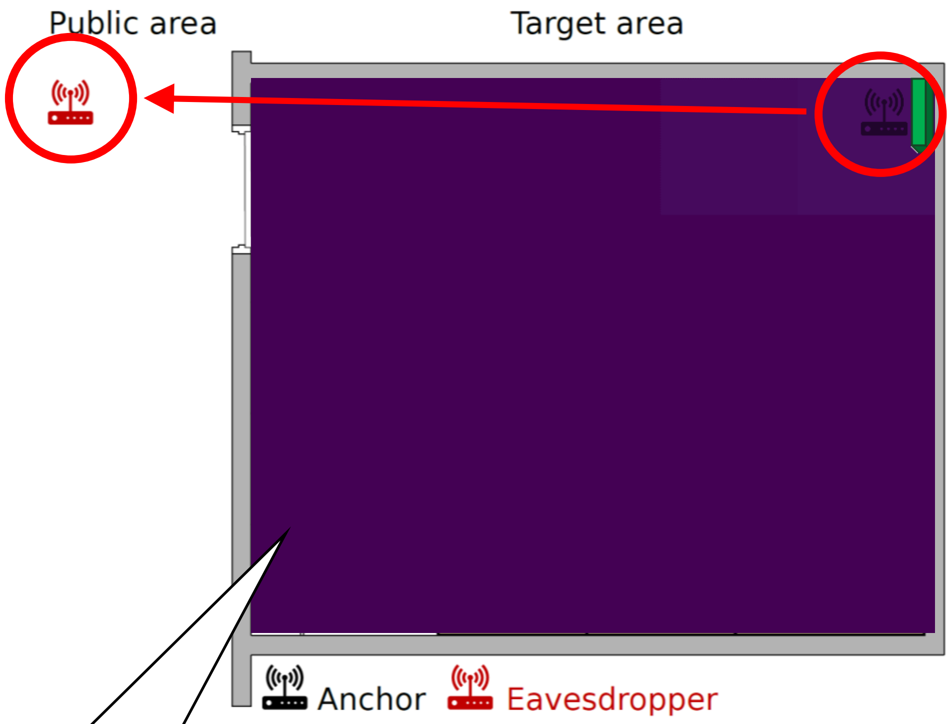
HEATMAP SETUP

Where **in the target area can the attacker detect motion?**



SPATIAL IMPACT OF IRSHIELD

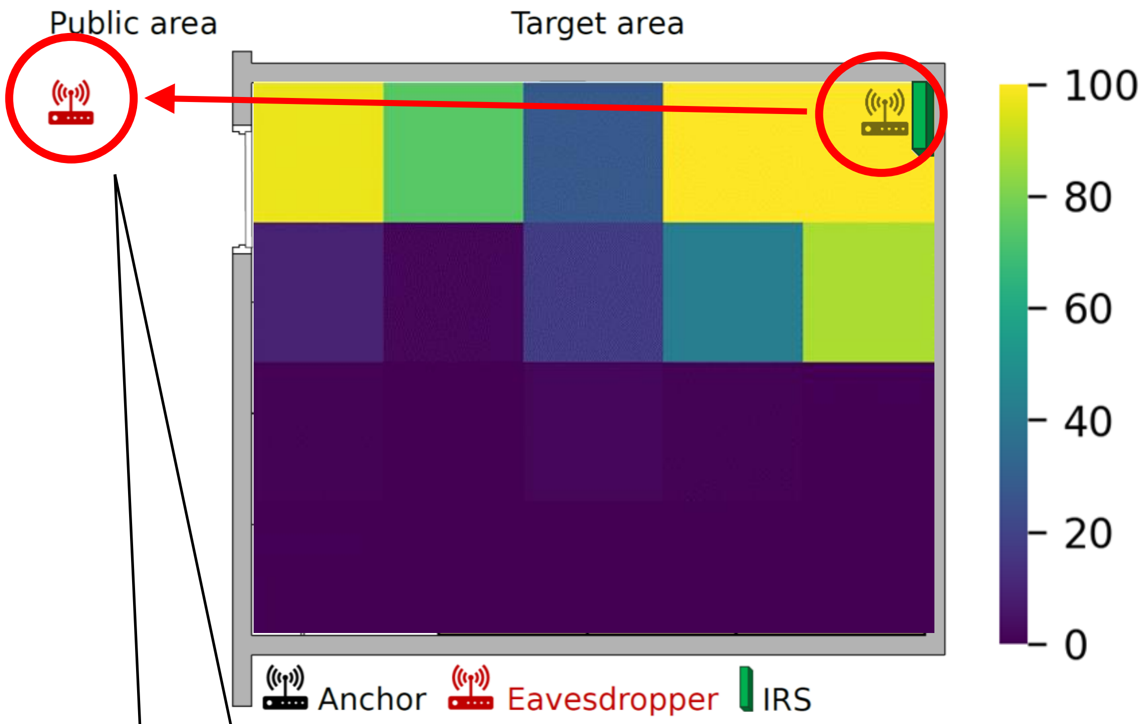
Motion detection according to the literature



Color shows detection rate in percent

With IRS

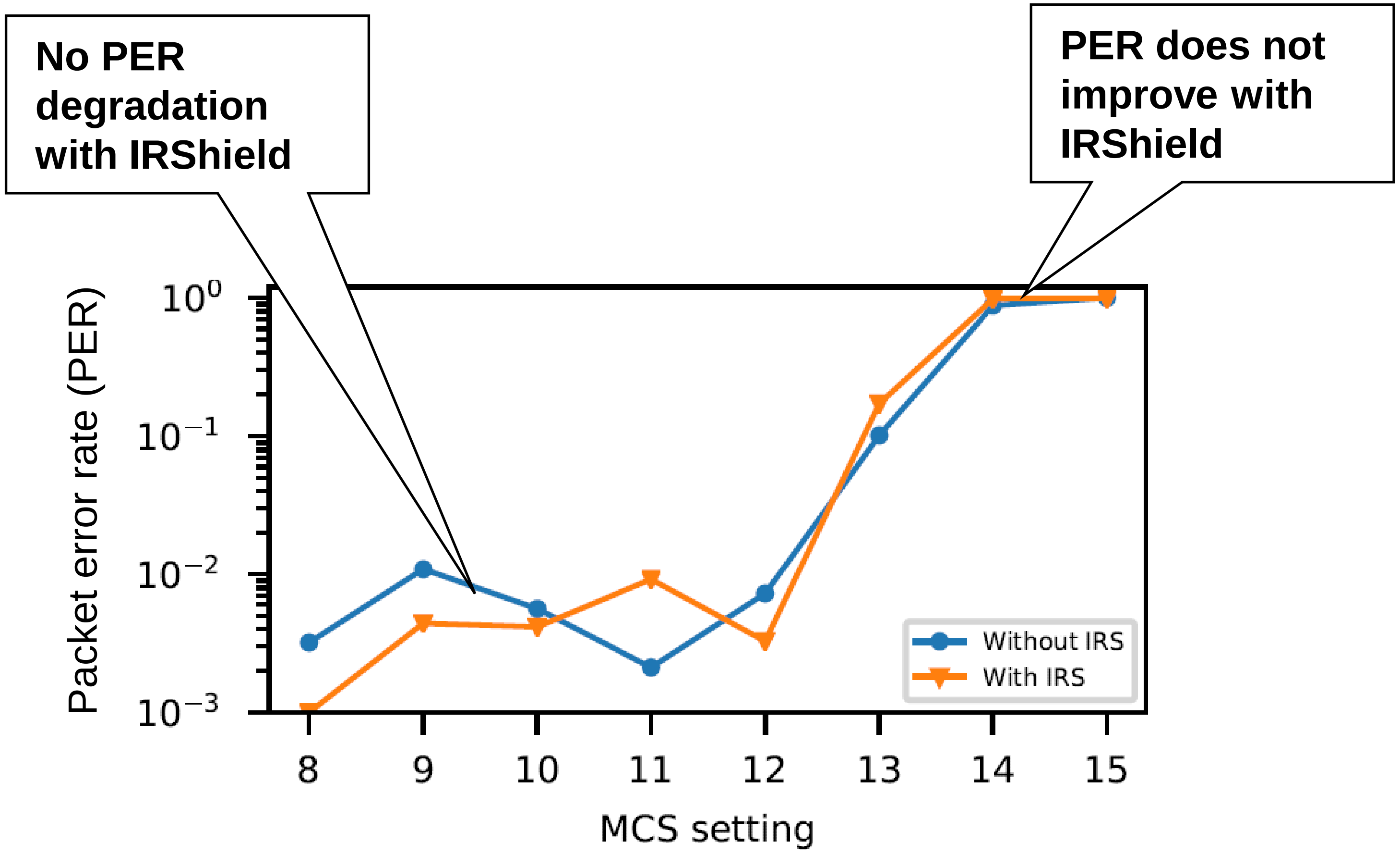
Adaptive motion detection



Attacker adapts to IRShield

With IRS

WIRELESS QUALITY OF SERVICE



Higher transmission speeds

FUTURE WORK

Verify IRShield effectiveness against additional wireless sensing attacks

Optimized IRS configurations to enhance impact of IRS on adversary channel

How to differentiate legitimate and adversarial wireless sensing?

How could a wireless sensing adversary benefit from using an IRS?

CONCLUSION

Wireless sensing and its privacy implications

IRS-based channel obfuscation to counter adversarial wireless sensing: IRShield

- Independent of devices, waveforms, and standards
- Plug-and-play operation
- No degradation of wireless quality-of-service

Evaluation against state-of-the-art human motion detection attack

Contact:
Paul Staat
paul.staat@mpi-sp.org

THANKS FOR YOUR ATTENTION!

Paper

https://arxiv.org/abs/2112.01967

Datasets

https://doi.org/10.5281/zenodo.6367411

Contact:

Paul Staat
paul.staat@mpi-sp.org