Building and Breaking Wireless Security

TECHNISCHE UNIVERSITÄT DARMSTADT

CROSSING

SEEMO SECURE MOBILE NETWORKING

Jiska Classen

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
jclassen@seemoo.tu-darmstadt.de
Tel.+49 6151 16-70924, Fax. +49 6151 16-70921
https://seemoo.de/jclassen

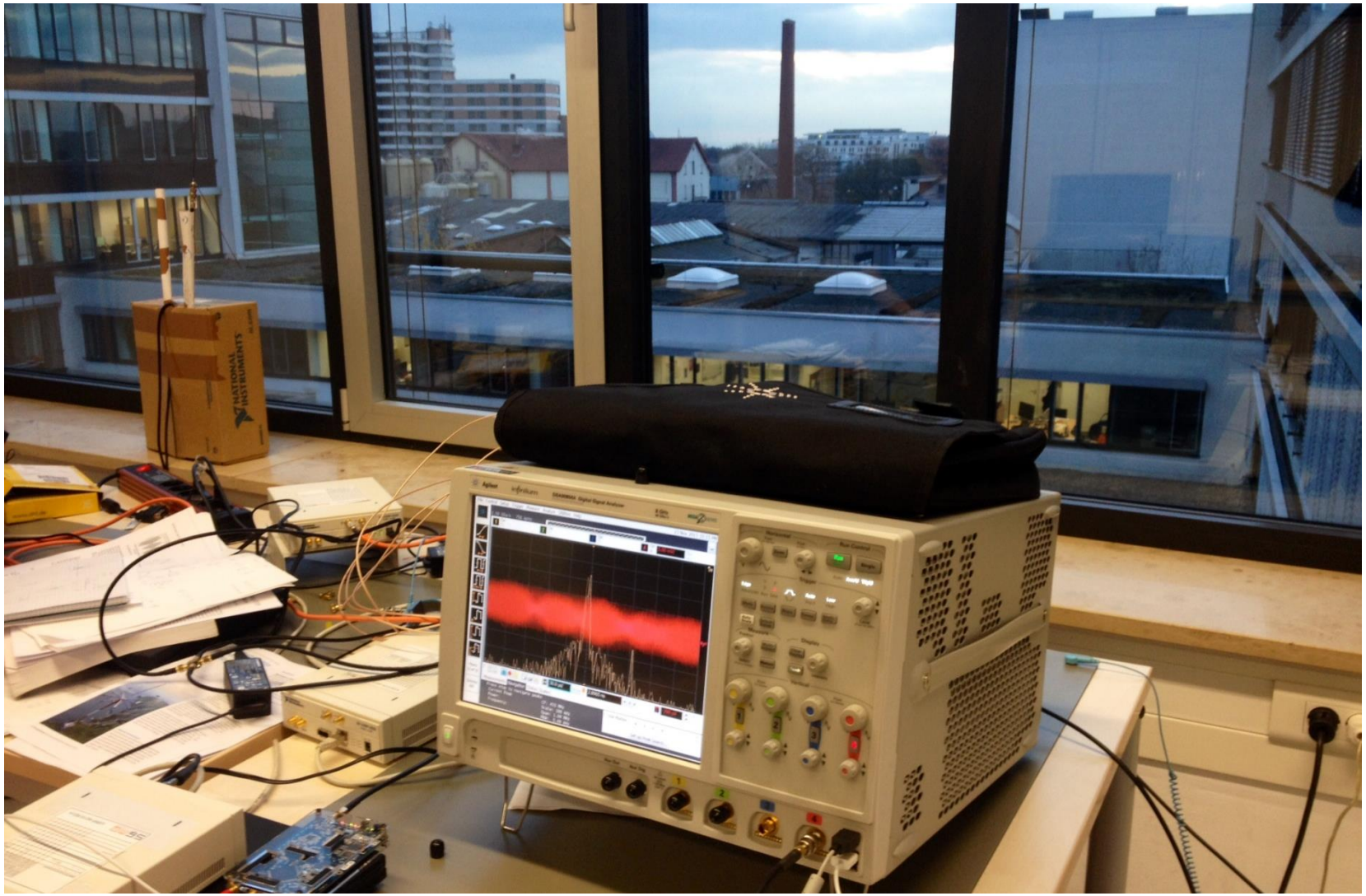
SEEMO DFG Deutsche Forschungsgemeinschaft CROSSING

Overview

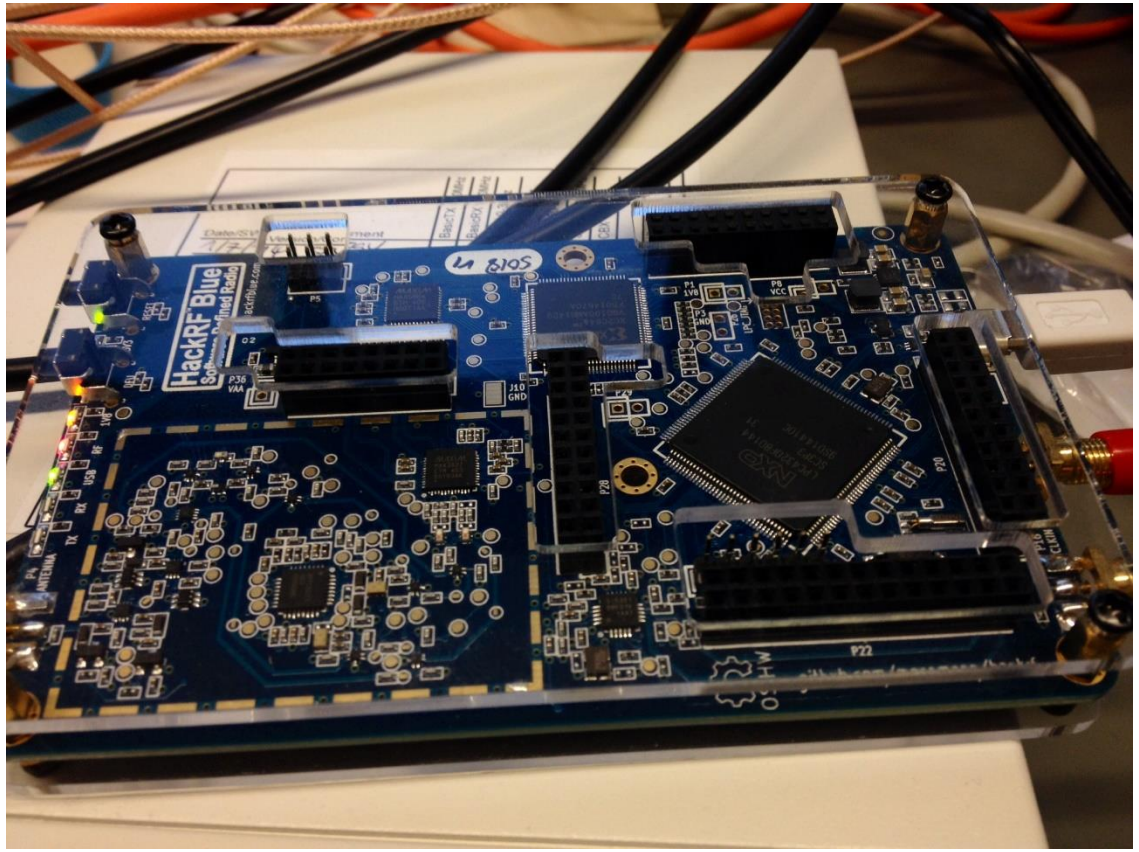
(1) Hardware
(2) Wireless Channels
(3) Breaking Wireless Security
(4) Building Wireless Security
(5) Getting Started

Hardware

Spectrum Analyzer or Oscilloscope

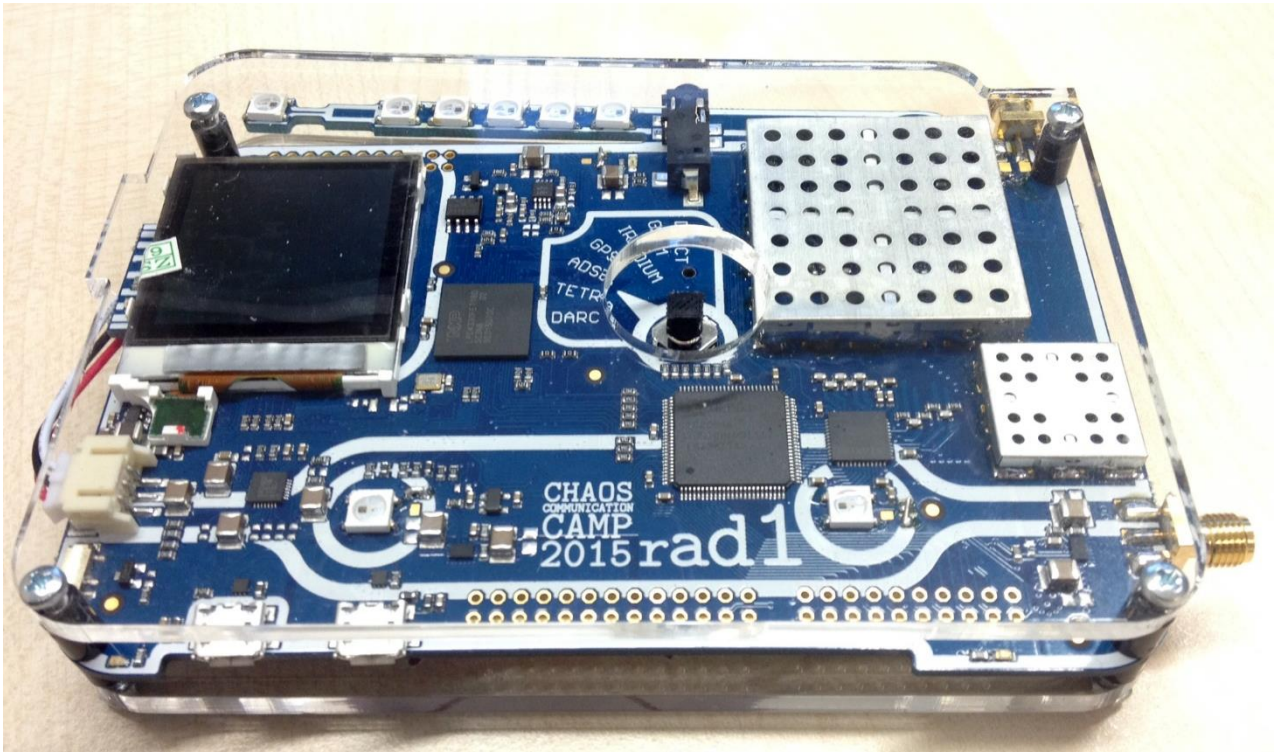


rad1o badge / HackRF



HackRF Blue

- Receiver and transmitter
- 1MHz-6GHz, 20Msps (**rad1o**: 1MHz-4GHz)
- 200€



DVB-T Sticks & rpitx

DVB-T Sticks

- Receiver for 53MHz-2.2GHz, ~2Msps
- 8€

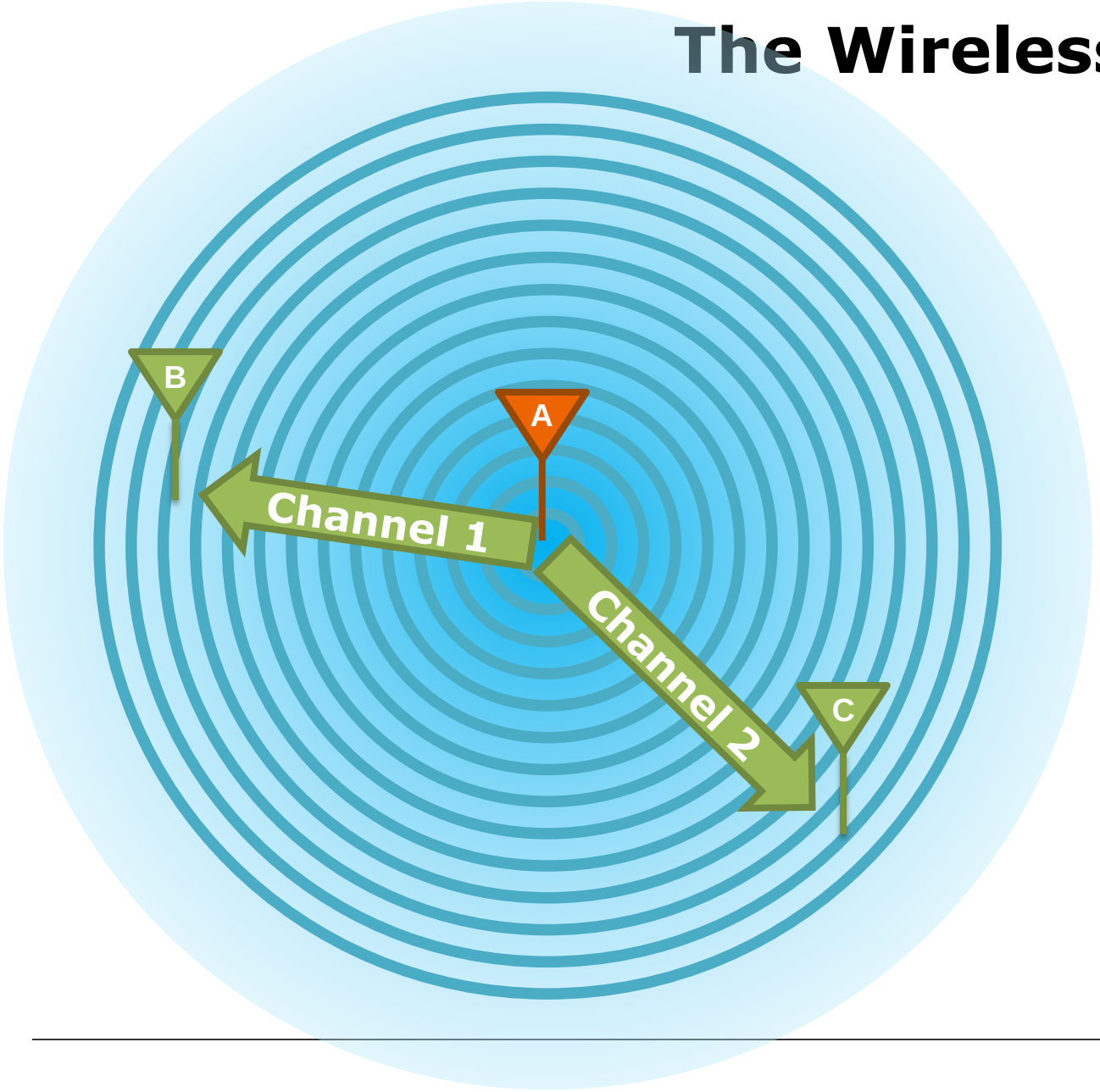
rpitx

- Cheap transmitter for Raspberry Pi (B, B+ and PI2)
- Use GPIO pins + long wire as antenna
- Low frequency signals: 130kHz-750MHz
- 35€

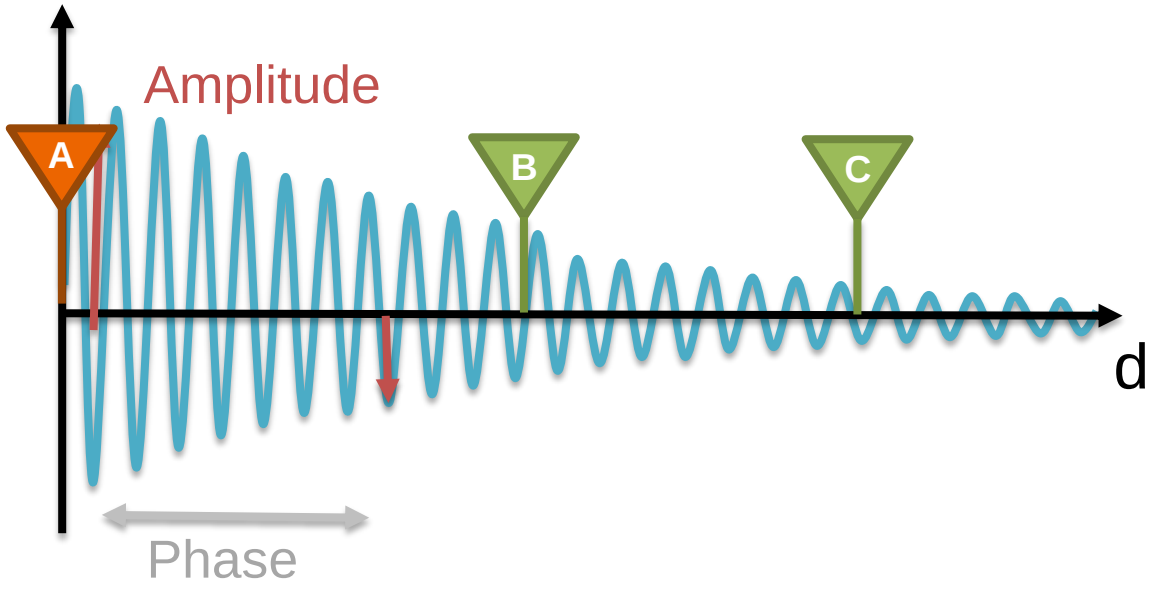
http://sdr.osmocom.org/trac/wiki/rtl-sdr
https://github.com/F5OEO/rpitx

Wireless Channels

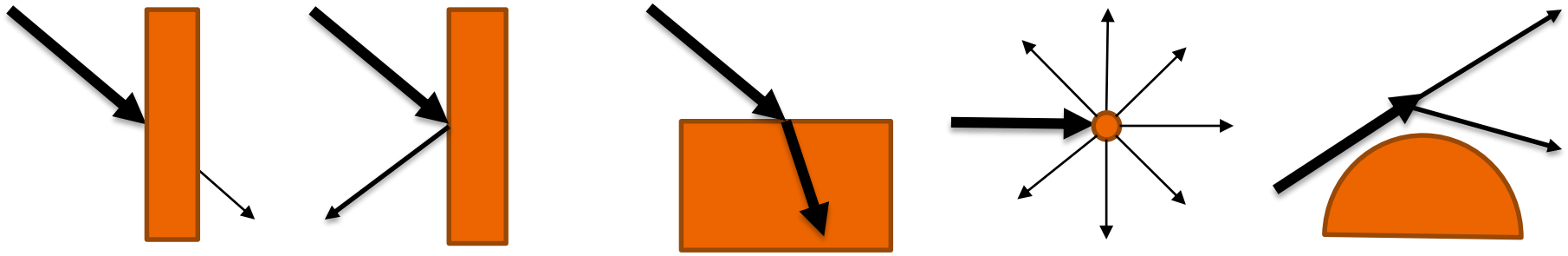
The Wireless Channel



- Every receiver has a **different channel** H
- H represents different **amplitude** and **phase** per frequency
- Channel **reciprocity**
- Time constraint: **speed of light**



Path Effects



- Channel impulse response (**time** domain)
- Channel frequency response (**frequency** domain)
- Transmitters, receivers, and objects move
  → **Frequency offset**

Breaking Wireless Security

Network Security

This is where the magic happens ☺

Cryptography
(Encryption, Signatures, …)

Bits

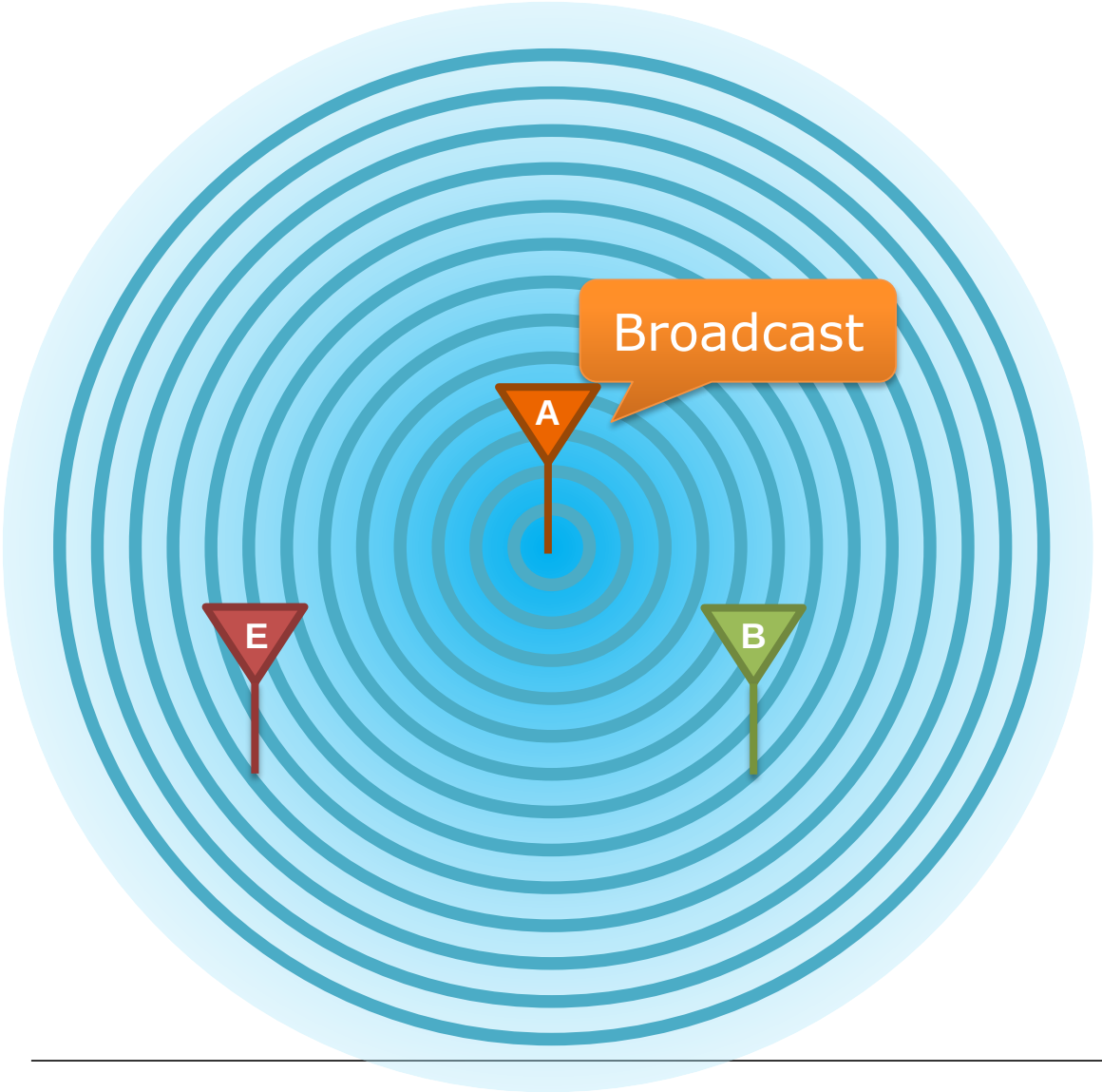
Waveform

I guess we need this?

Weird stuff but nobody would attack it!!!

https://www.flickr.com/photos/84568447@N00/3019772338

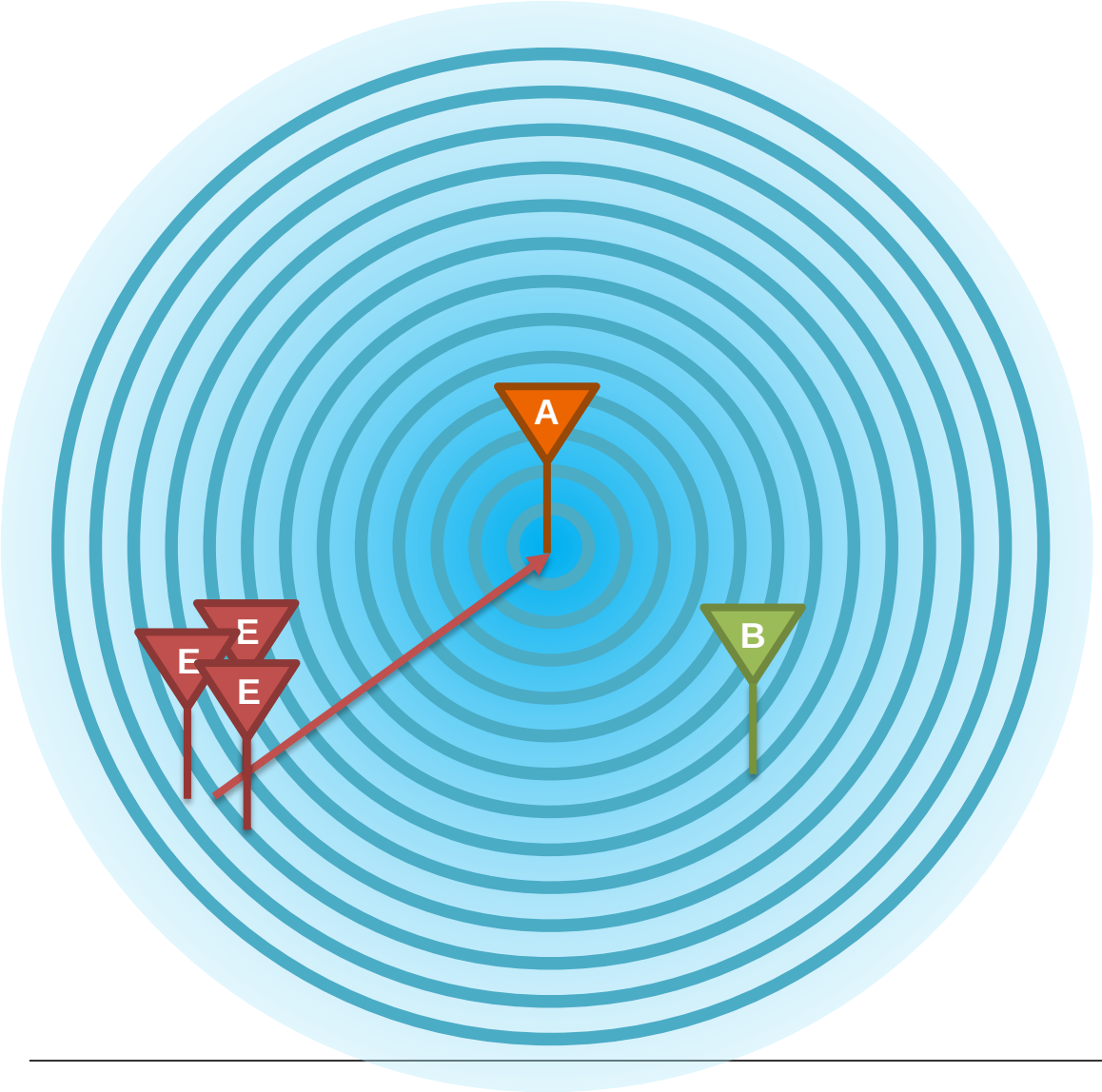
Wireless Transmissions



- Everybody within the transmission range can **eavesdrop**

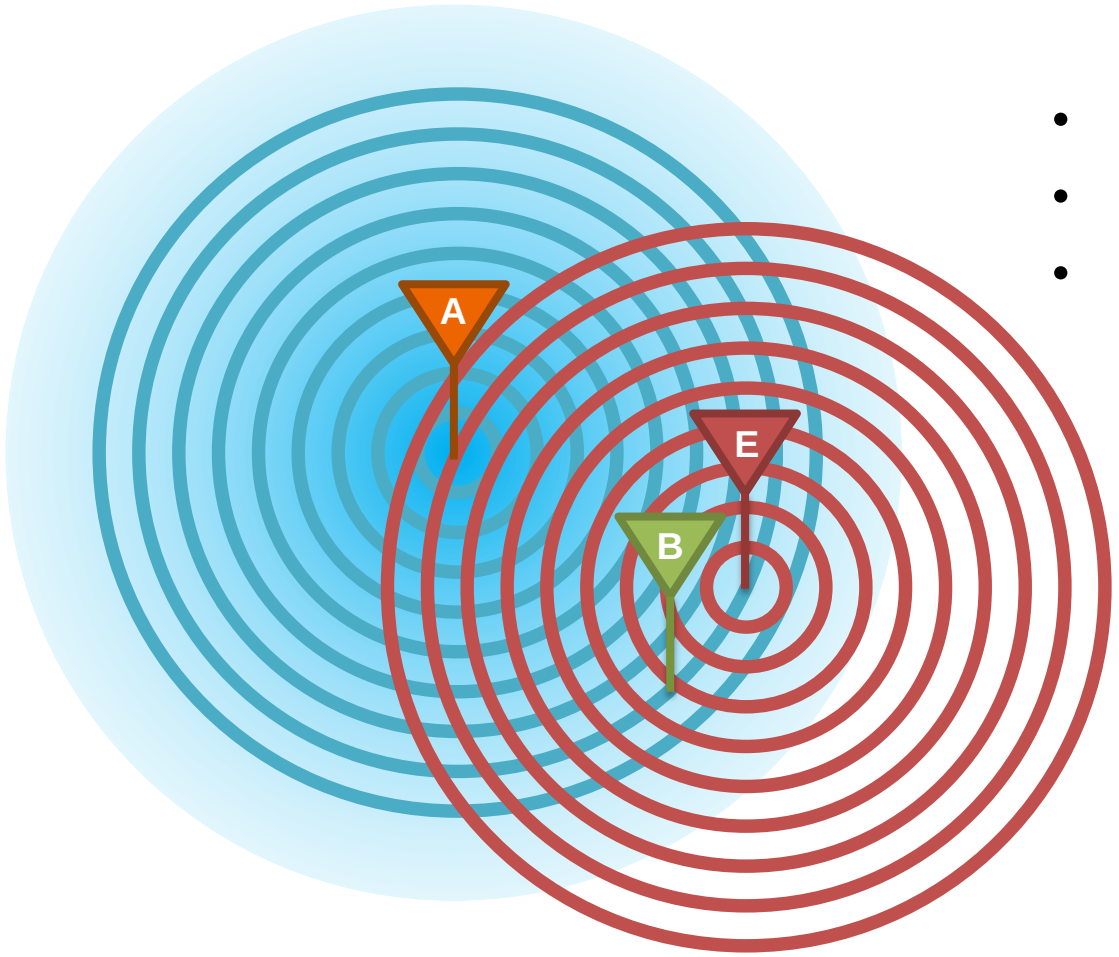
20 years later…

Wireless Transmissions



- Everybody within the transmission range can **eavesdrop**
- Signal sources can be **located** (privacy!)
- Signal reception range can be **enhanced**

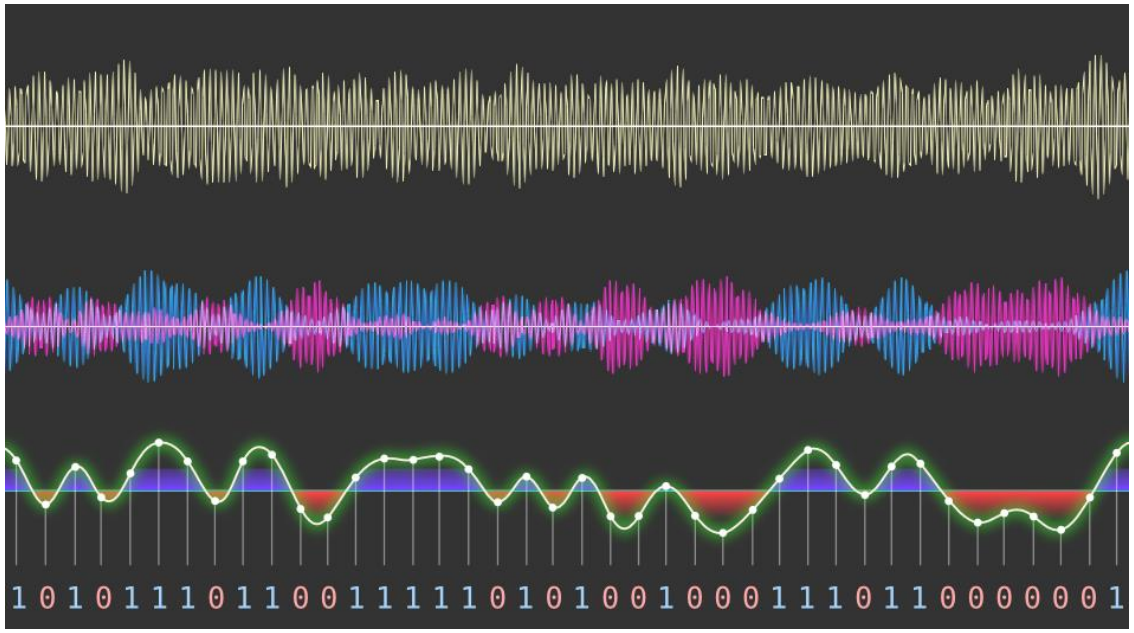
Wireless Transmissions

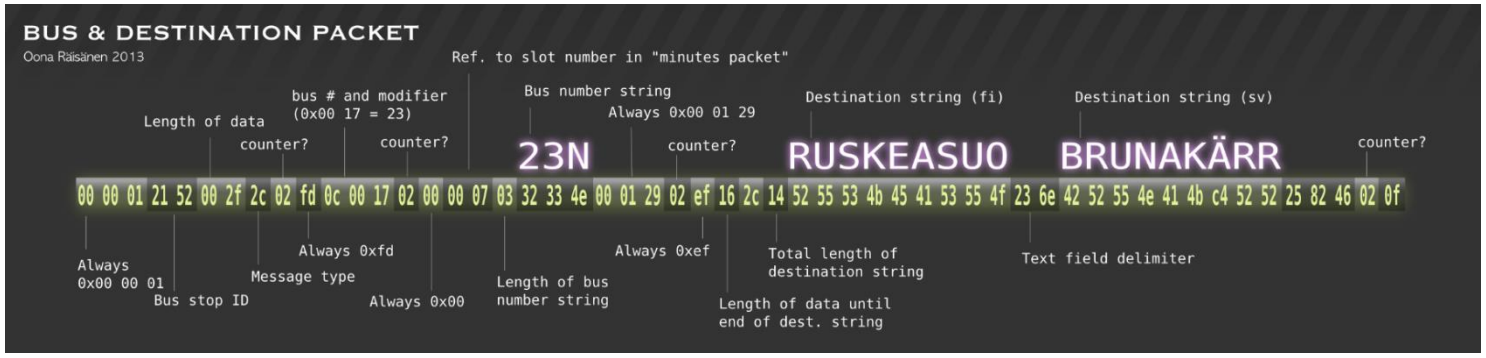


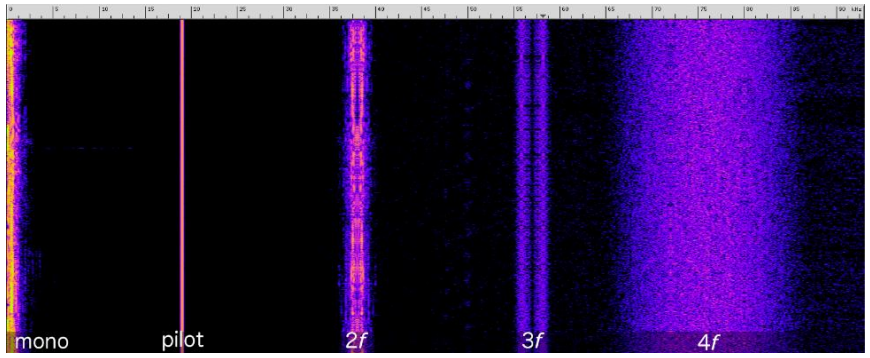
- Everybody within the transmission range can **eavesdrop**
- Signal sources can be **located** (privacy!)
- Signal reception range can be **enhanced**
- Signals can be **injected**

Protocol Reverse Engineering
Bus Stop Display

- Capture wireless data with **gqrx** or **baudline**
- Find out the modulation scheme, e.g. by analyzing your capture in **audacity**
- …now we have the bits ☺
- Reverse engineer their meaning
  → Oona did that on 30C3:
  "My journey into FM-RDS"



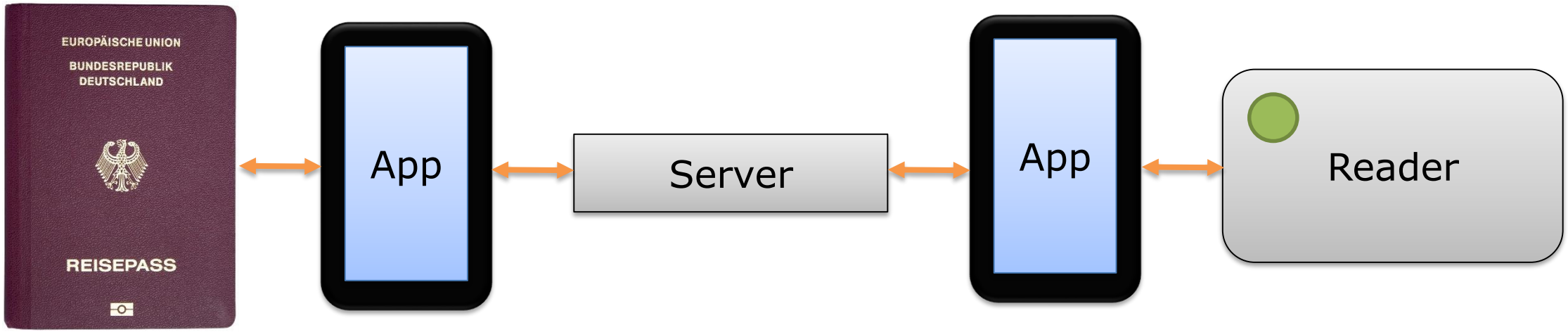




http://www.windytan.com/2013/11/decoding-radio-controlled-bus-stop.html
http://www.bastibl.net/reversing-bus-telemetry/

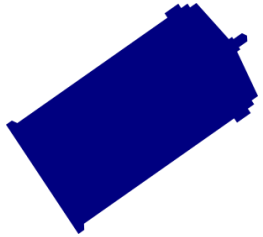
NFC Wormholing

- **Assumption**: passport and reader are in close proximity, because wireless transmissions have a **limited range**
- **Problem**: **forwarding** requests and replies is possible

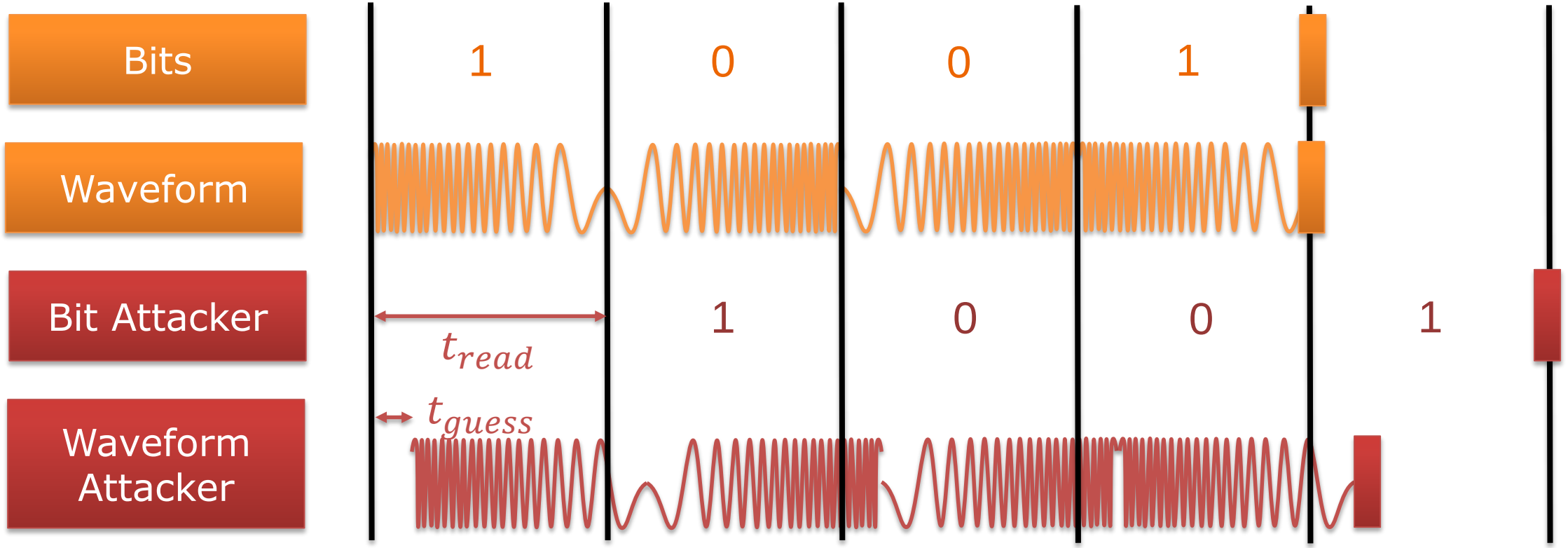


- Time constraint: speed of light!
  $50\,ms \;\widehat{=}\; 14990\,km$

Wormholing & Time Traveling



- Signal propagation is limited by speed of light ☺
- Wormholing protection: check for round trip time of single bits (**distance bounding**)
- Problem: **early detection** of actual bit values in the waveform

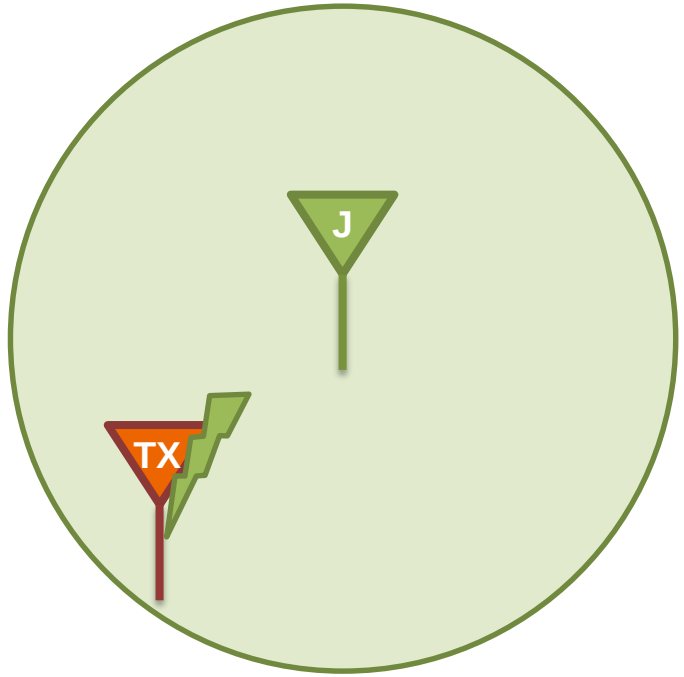


Reactive Jamming

- WiFi: CSMA/CA
- Selectively jam other WiFi stations
  → increased contention window
- Use minimal contention window for yourself ☺
- Just $15 WiFi dongle with modified firmware

Friendly Jamming for Confidentiality

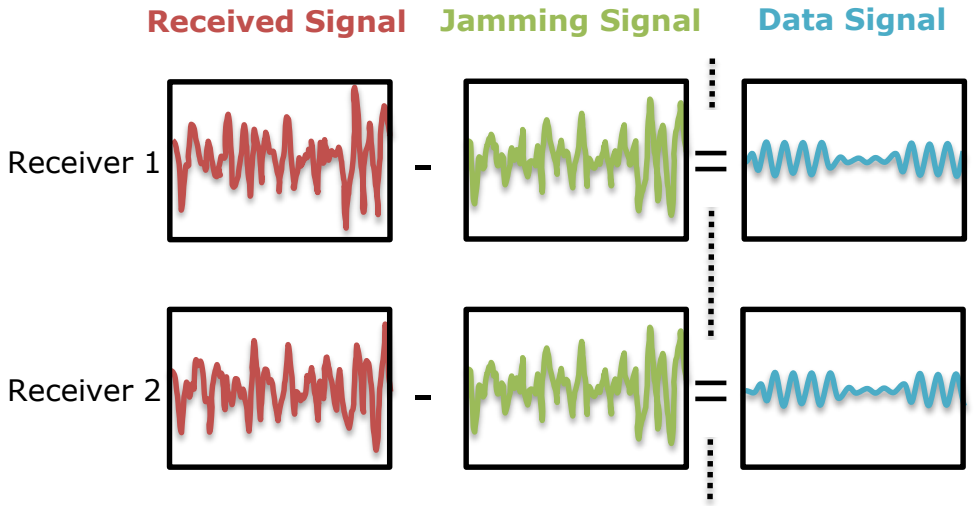
- Disable communication of others via jamming

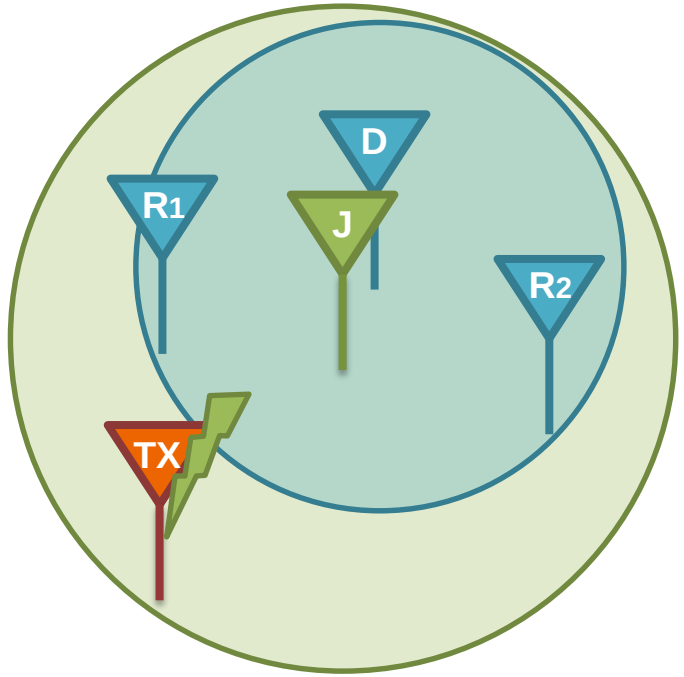


W. Shen, et al. "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time." *S&P 2013.*
Tippenhauer, Nils Ole, et al. "On limitations of friendly jamming for confidentiality." *S&P 2013.*

Friendly Jamming for Confidentiality

- Disable communication of others via jamming
- Filter out jamming pattern to communicate anyway
  → Build **authorization and confidentiality**



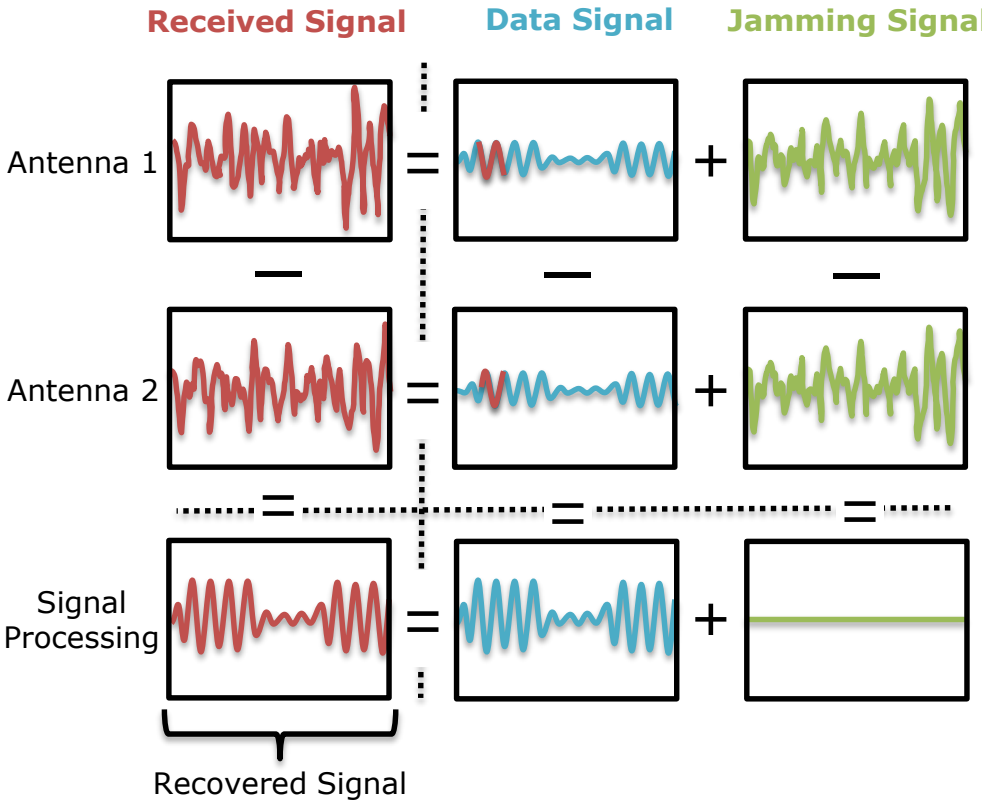


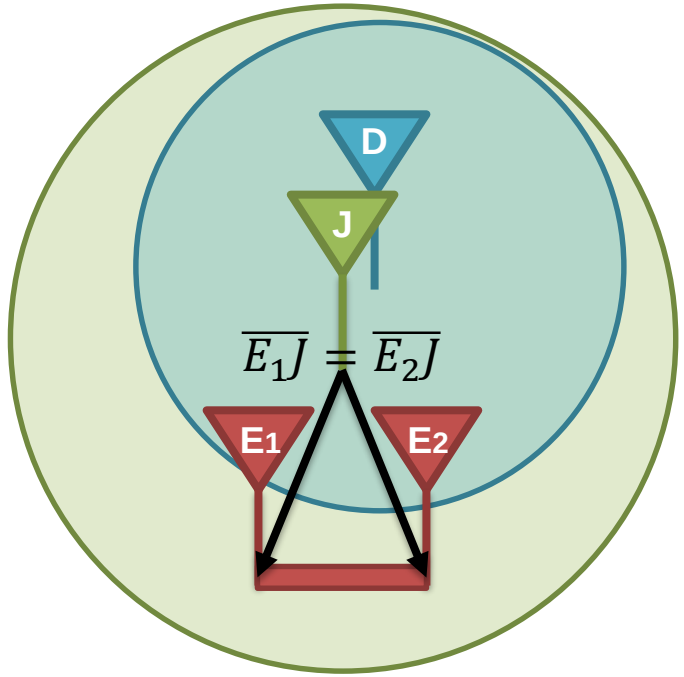
pseudo-random jamming

W. Shen, et al. "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time." *S&P 2013.*
Tippenhauer, Nils Ole, et al. "On limitations of friendly jamming for confidentiality." *S&P 2013.*

Friendly Jamming Vulnerability

- Disable communication of others via jamming
- Filter out jamming pattern to communicate anyway
- **Problem:** Multi-antenna receivers can also filter out the jamming pattern



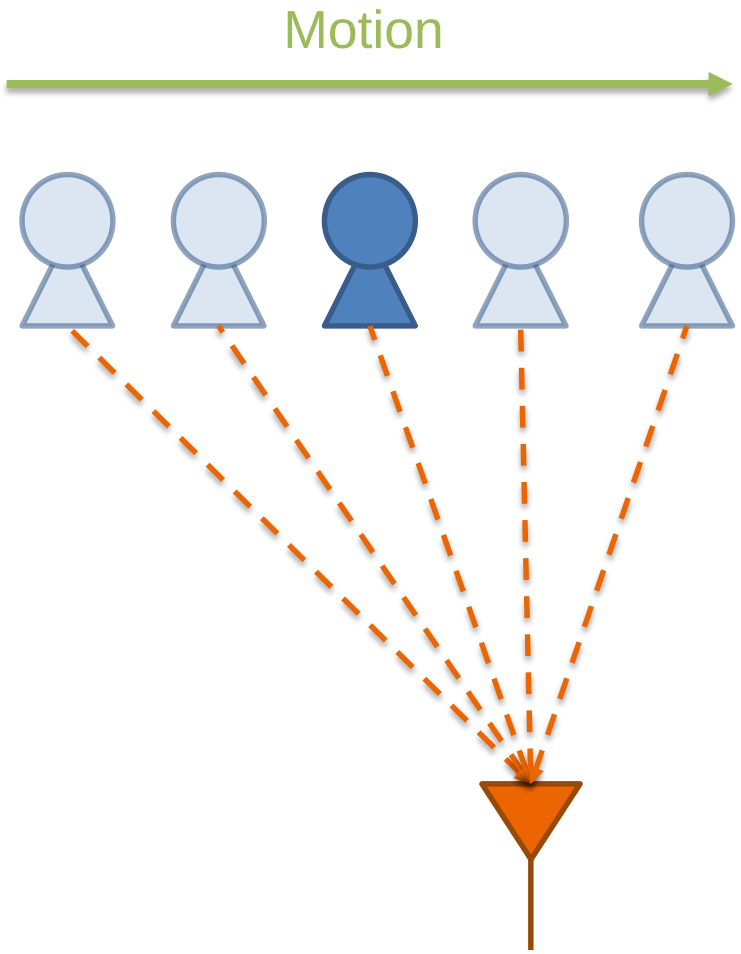


equal channel attacker

W. Shen, et al. "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time." *S&P 2013.*
Tippenhauer, Nils Ole, et al. "On limitations of friendly jamming for confidentiality." *S&P 2013.*

Seeing with Wi-Fi

2.4GHz Radar



Single, stationary antenna

- **Channel** measurements contain **reflections** and other path effects
- Filter out reflections from the static building
- **Identify and track humans**
- Gesture-based communication through walls
- **Single antenna** instead of antenna array based on ISAR: motion over time, channel reciprocity

Adib, Fadel, and Dina Katabi. “See through walls with WiFi!” *Sigcomm 2013.*

Hearing with Wi-Fi

Mouth Eavesdropping & Vibrometry

- Track lip movements to hear through walls
- Track loudspeaker movements
- Track Wi-Fi chip vibrations caused by audio on a smartphone

Wang, Guanhua, et al. "We can hear you with Wi-Fi!." *Mobicom 2014.*
Wei, Teng, et al. "Acoustic Eavesdropping through Wireless Vibrometry." *Mobicom 2015.*

Building Wireless Security

Wireless Physical Layer Security

Cryptography

Bits

Waveform

Let's do the magic here ☺

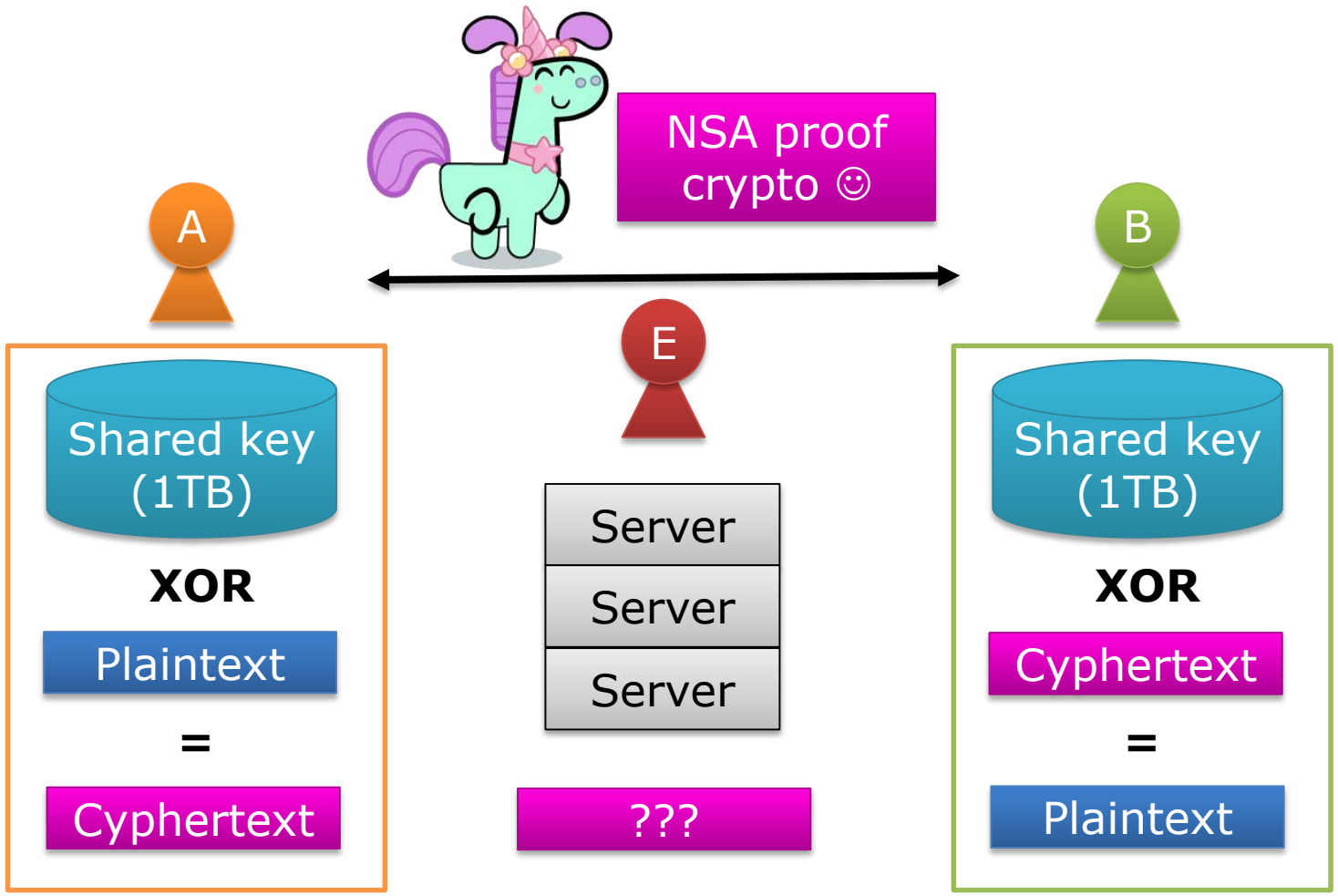
https://www.flickr.com/photos/84568447@N00/3019772338

Information-Theoretic Security

Confidentiality

!= computational security

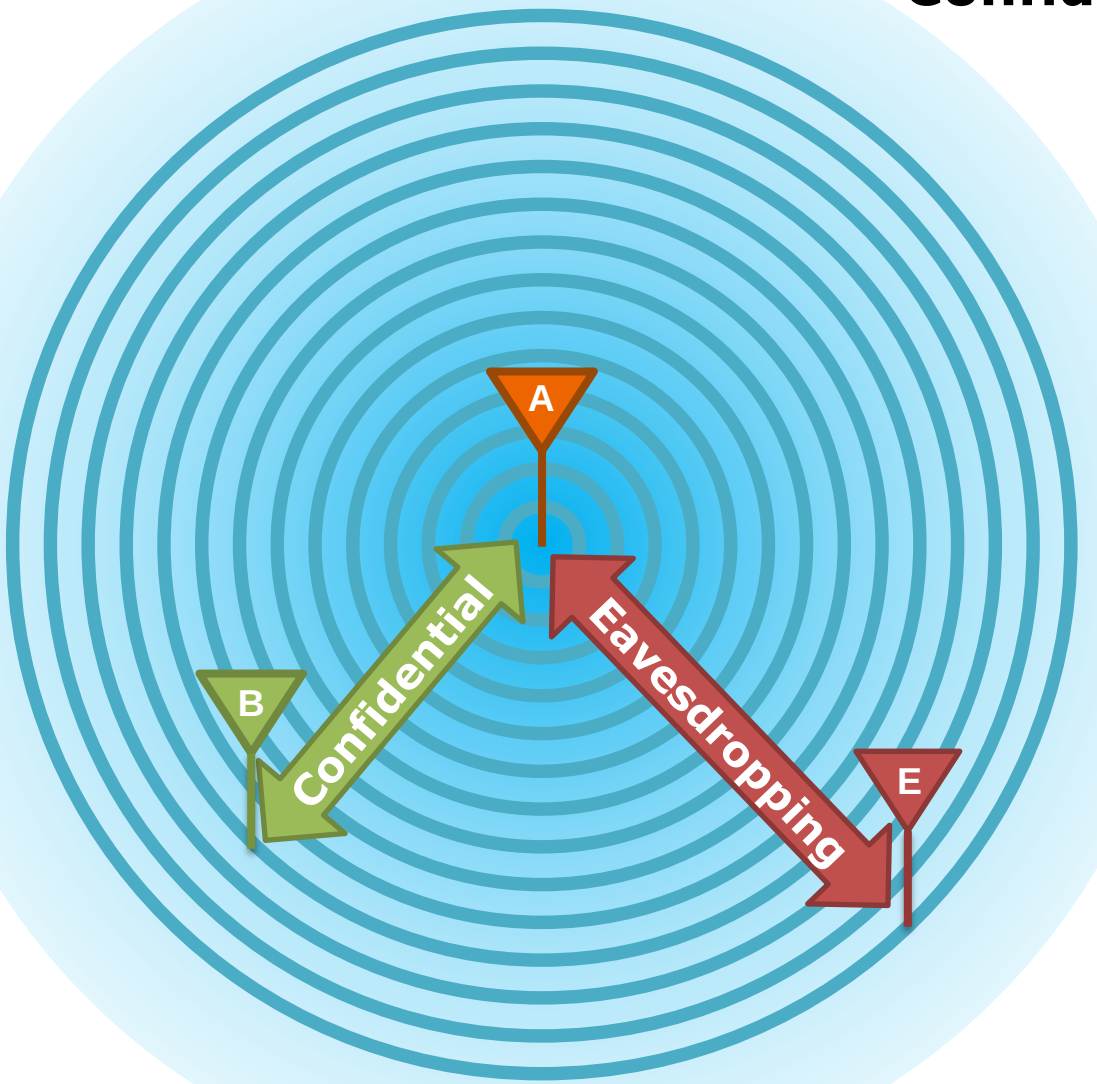
- **Unlimited computing power does not help attackers**
- Information-theoretic security in encryption: **one-time pad**



https://www.flickr.com/photos/84568447@N00/3019772338

Wyner's Wiretap Channel

Confidentiality



Information-theoretic security:

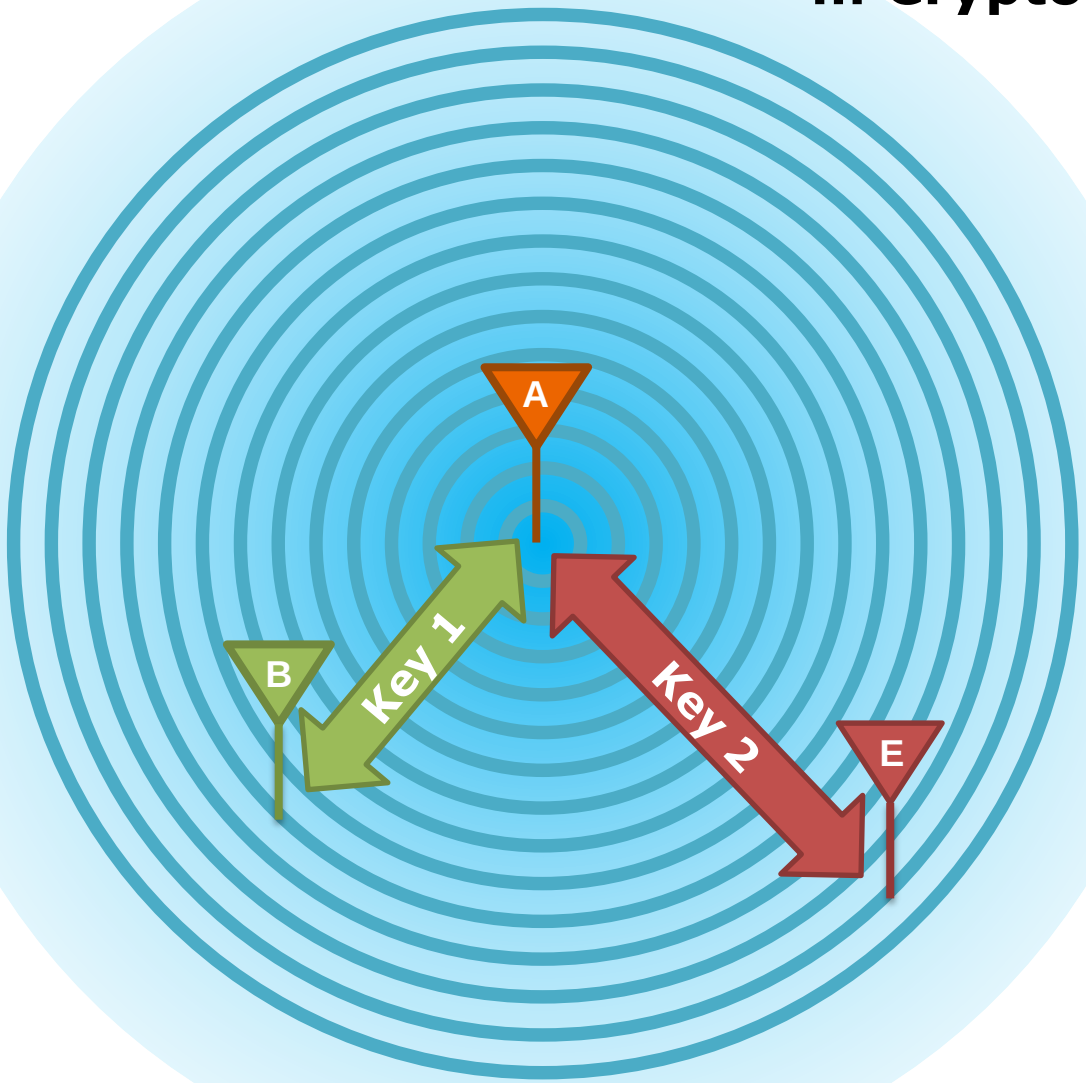
- Every receiver has a **different channel** H
- If H_{AB} is better than H_{AE}, Eve gets less information
- Use **Bob's advantage** for **confidential** information

Practical problems!

- H_{AE} unknown
- Eve can get more/better antennas

Key Extraction

… Cryptography Basis



- Every receiver has a **different channel** H
- Channel **reciprocity** helps to extract **symmetric keys**

Typical **implementation weaknesses:**

- Some metrics like received signal strength are not random enough (just 8 bit value & predictable)
- Reproducability for fixed stations

Jana, Suman, et al. "On the effectiveness of secret key extraction from wireless signal strength in real environments." *Mobicom 2009.*

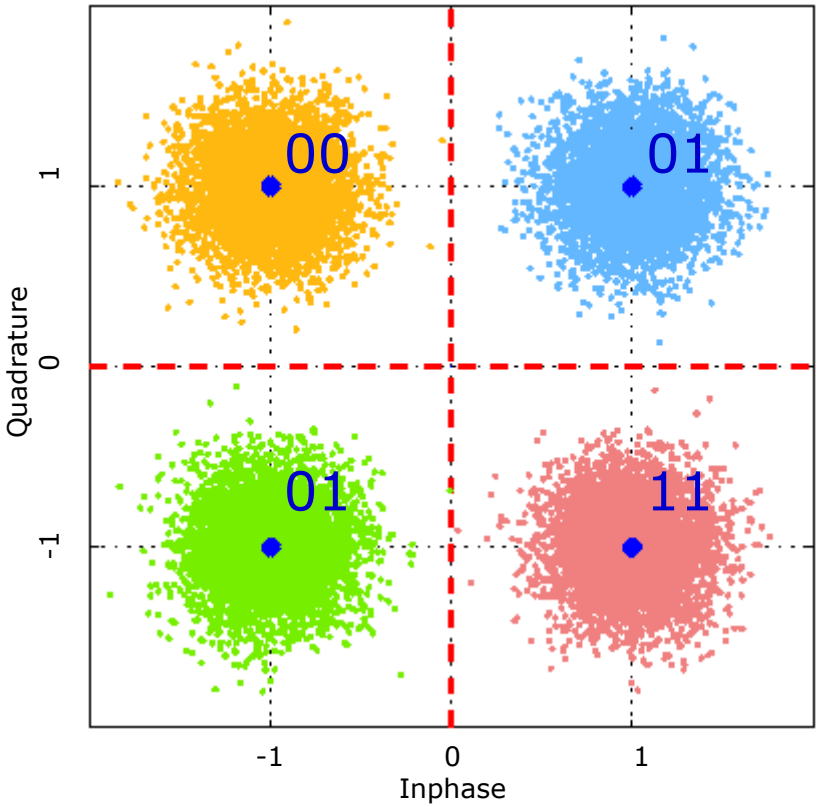
Covert Channels

Information Hiding, Confidentiality

- Noise is normal in wireless signals
- Noise gets compensated in upper layers
- Hide information in wireless noise

Practical problems:

- Ensure no possibility to uncover the covert channel at **upper layers** (e.g. increased frame error rate)
- **Statistical** inconspiciousness



- **sent constellation**
- **received, noisy constellation**

Distance Bounding

Authentication, Authorization

- Signals cannot travel faster than **speed of light**
- Measure round trip time and cryptographically secure it

Hancke, Gerhard P., and Markus G. Kuhn. "An RFID distance bounding protocol." *SecureComm 2005.*

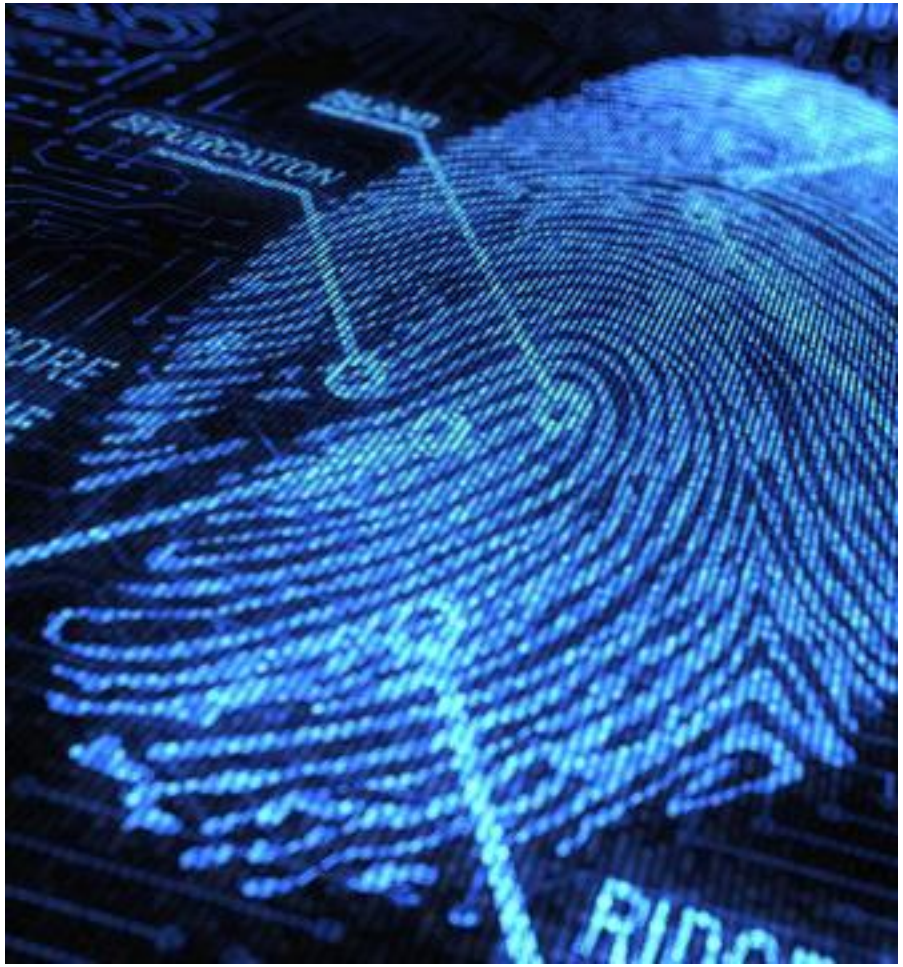
Device Fingerprinting

Authentication, Authorization

- **Identification** of single devices
- **Classification** of device types
- Device-specifics per **harware** vendor (exclude third party devices from a network)

Problem:

- Low-end receiver fingerprints can be **faked** with software-defined radios

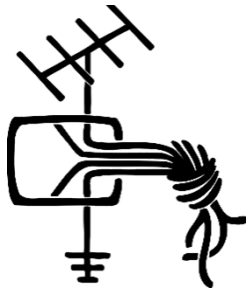


S. Rehman et al. "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers." *Journal of Computer and System Sciences 2014.*

Where to start?

Getting Started

- **Chaoswelle** / D23
- **rad1o** assembly



- Get a **ham radio license** („Amateurfunk-Lizenz“)

- Record signals and **ask** the experts

- **Lectures** etc. offered by SEEMOO / TU Darmstadt
- Maybe your university also offers something ☺
  The **AkadAFU** people are working on this!

Q&A