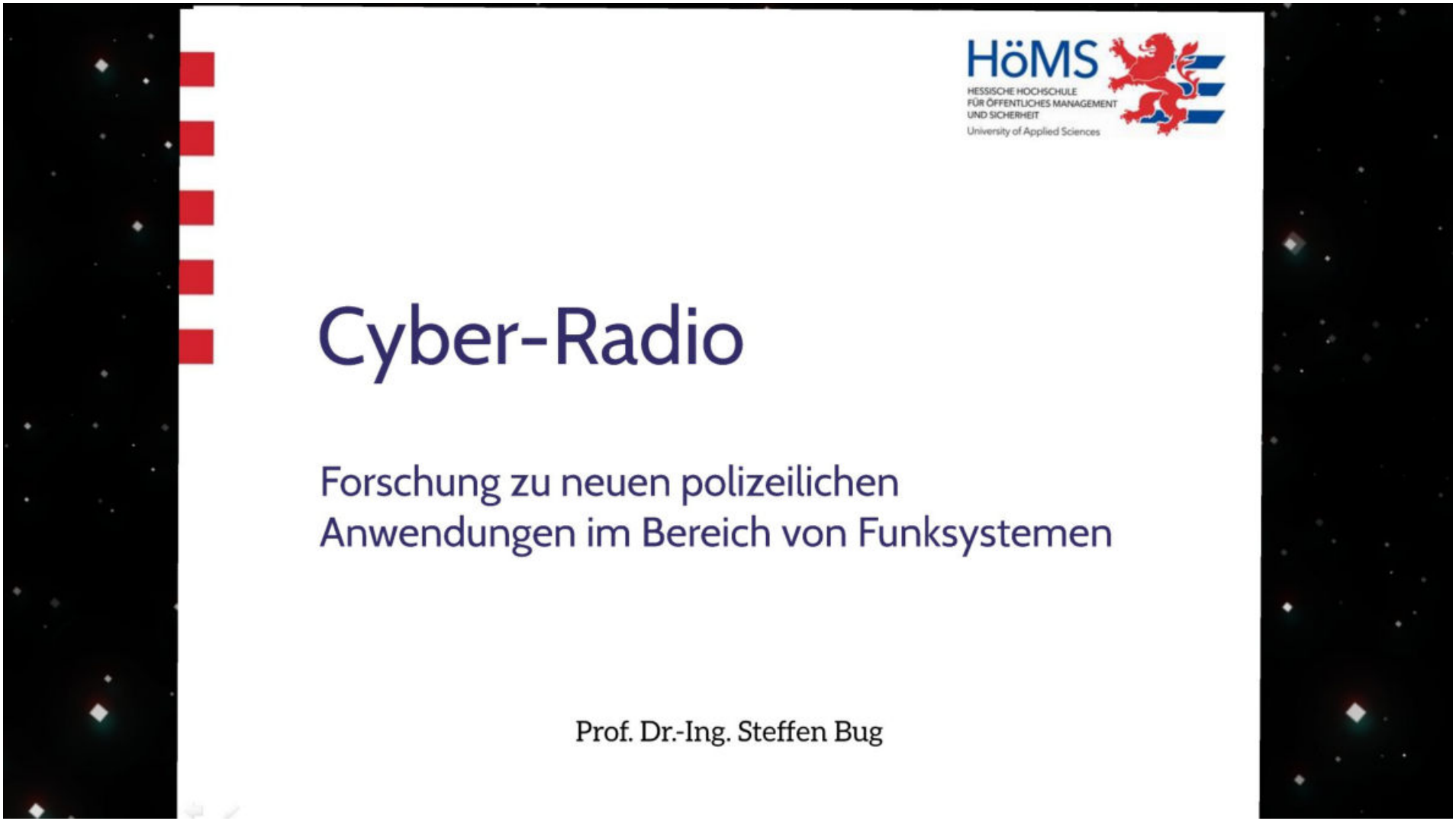

HöMS
HESSISCHE HOCHSCHULE
FÜR ÖFFENTLICHES MANAGEMENT
UND SICHERHEIT
University of Applied Sciences
Cyber-Radio

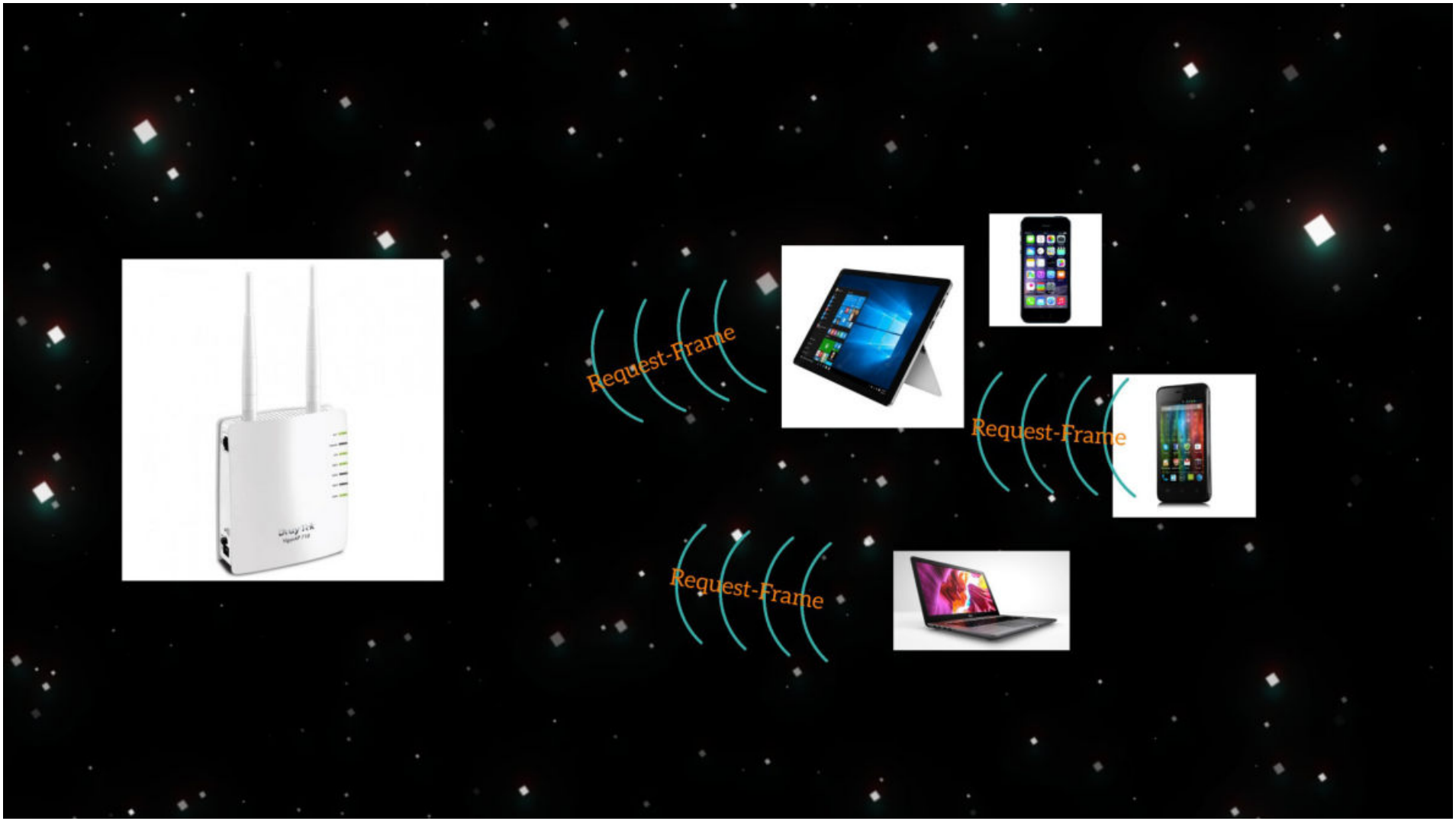

1080


Zur "Beobachtung" eignet sich selbstredend das sichtbare Spektrum elektromagnetischer Wellen
... aber nicht nur!


Auch für uns unsichtbare
elektromagnetische Wellen bieten einen
Beobachtungsnutzen

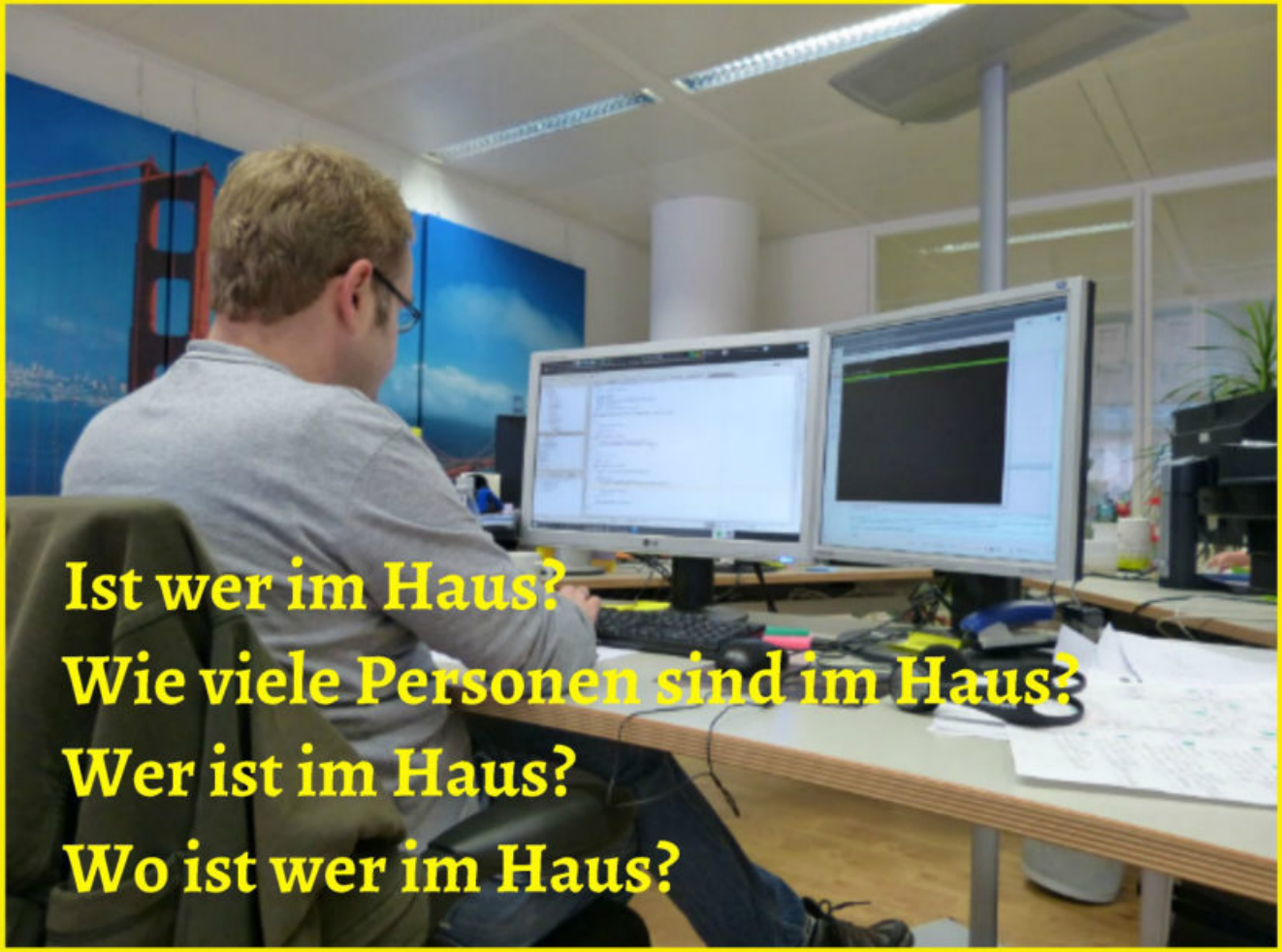

HöMS
HESSISCHE HOCHSCHULE
FÜR ÖFFENTLICHES MANAGEMENT
UND SICHERHEIT
University of Applied Sciences
Cyber-Radio
Forschung zu neuen polizeilichen
Anwendungen im Bereich von Funksystemen
Prof. Dr.-Ing. Steffen Bug


Beacon-Frames


Request-Frame
Request-Frame
Request-Frame


Beacon-Frames
passives Mitschneiden möglich!!!
Request-Frame
Request-Frame
Request-Frame


HAUS


Ist wer im Haus?
Wie viele Personen sind im Haus?
Wer ist im Haus?
Wo ist wer im Haus?

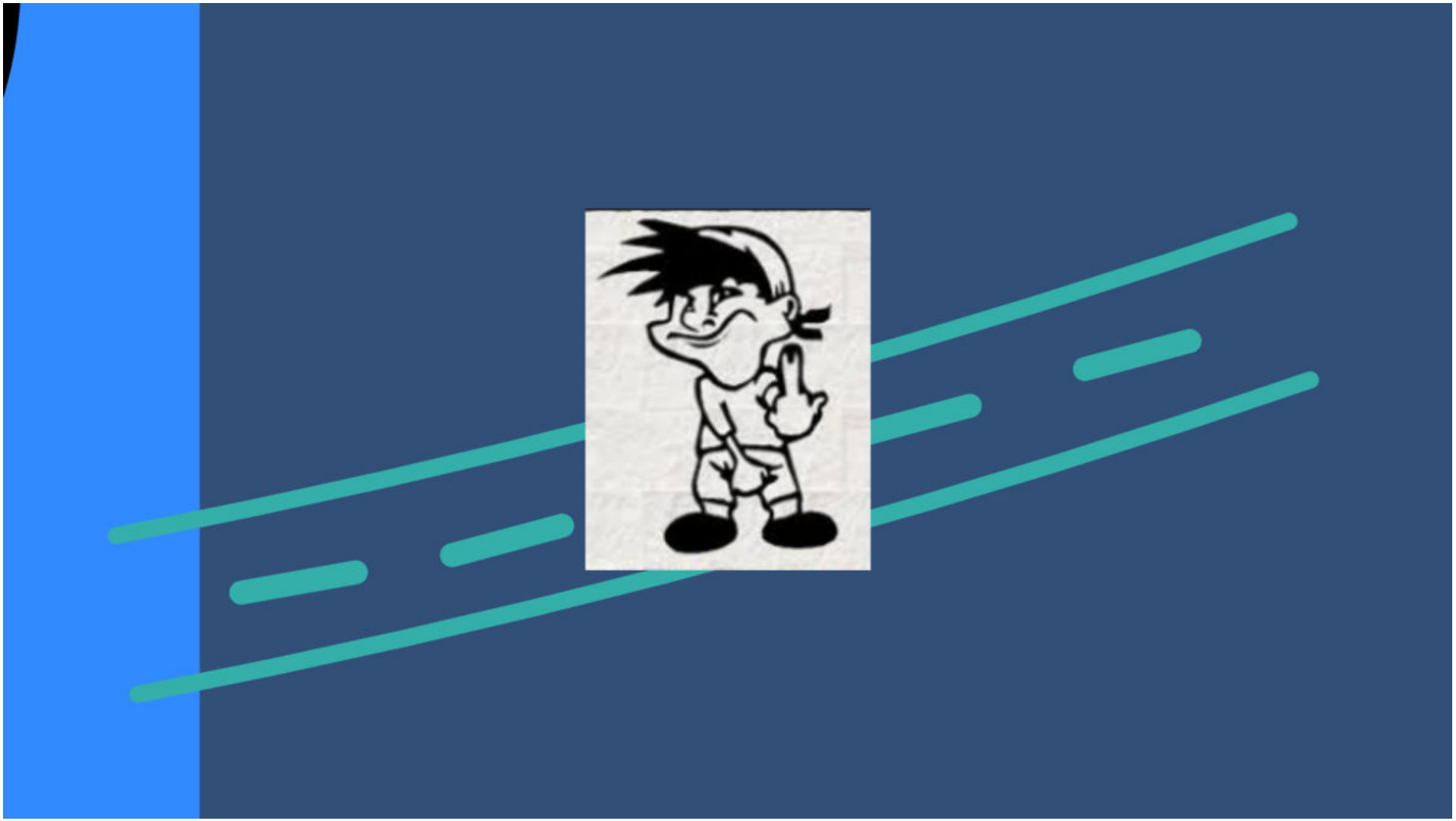

WLAN-Frame
POLIZEI


GAUNER-ALLEIN IM HAUS


GAUNER-ALLEIN IM HAUS

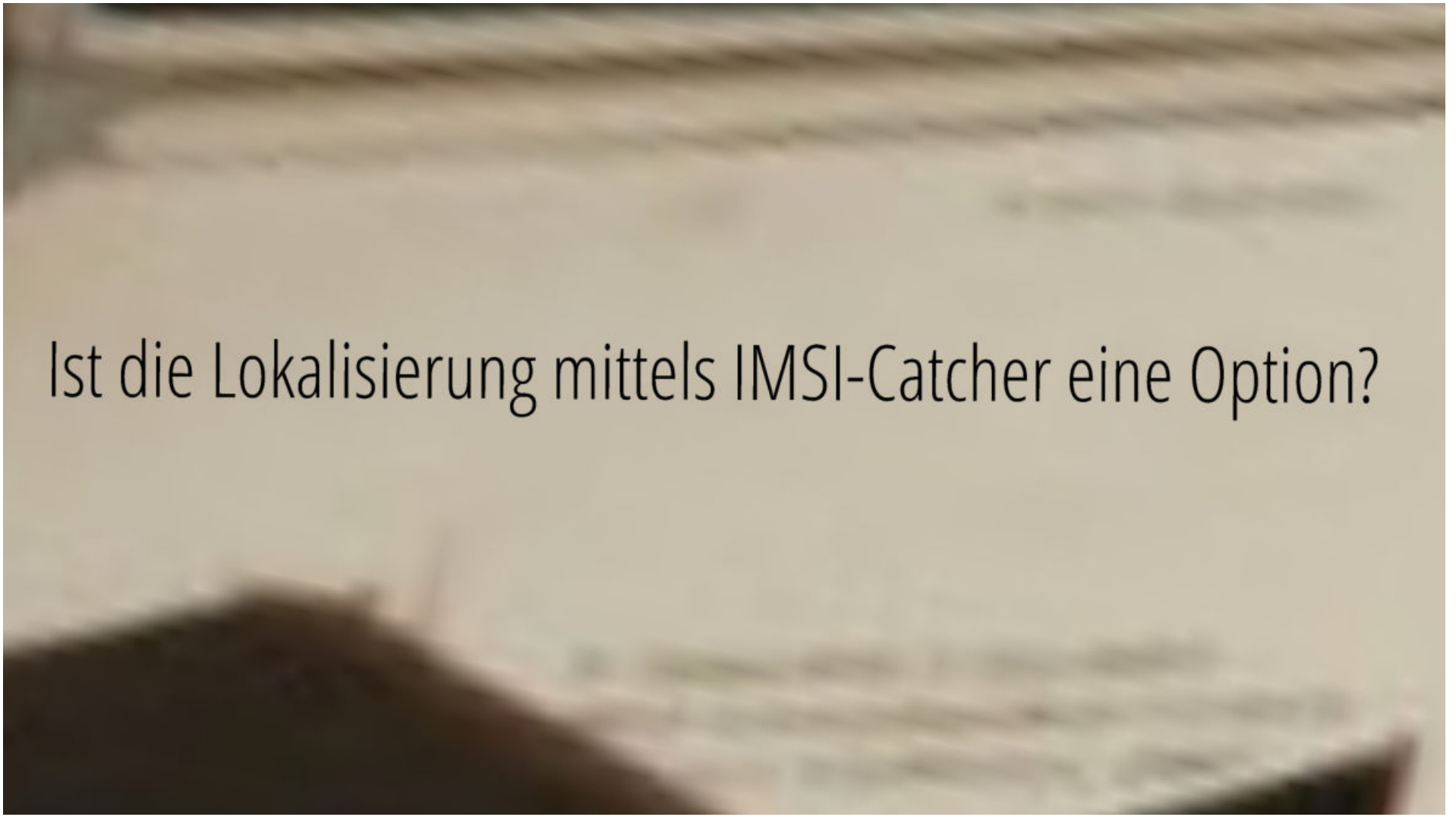

GAUNER-ALLEIN IM großen HAUS
... aber wo???


GAUNER-ALLEIN
großen HAUS
... aber wo???




HöMS
HESSISCHE HOCHSCHULE
FÜR ÖFFENTLICHES MANAGEMENT
UND SICHERHEIT
University of Applied Sciences


HöMS


Ist die Lokalisierung mittels IMSI-Catcher eine Option?

Cell Site Simulator
IMSI-Catcher

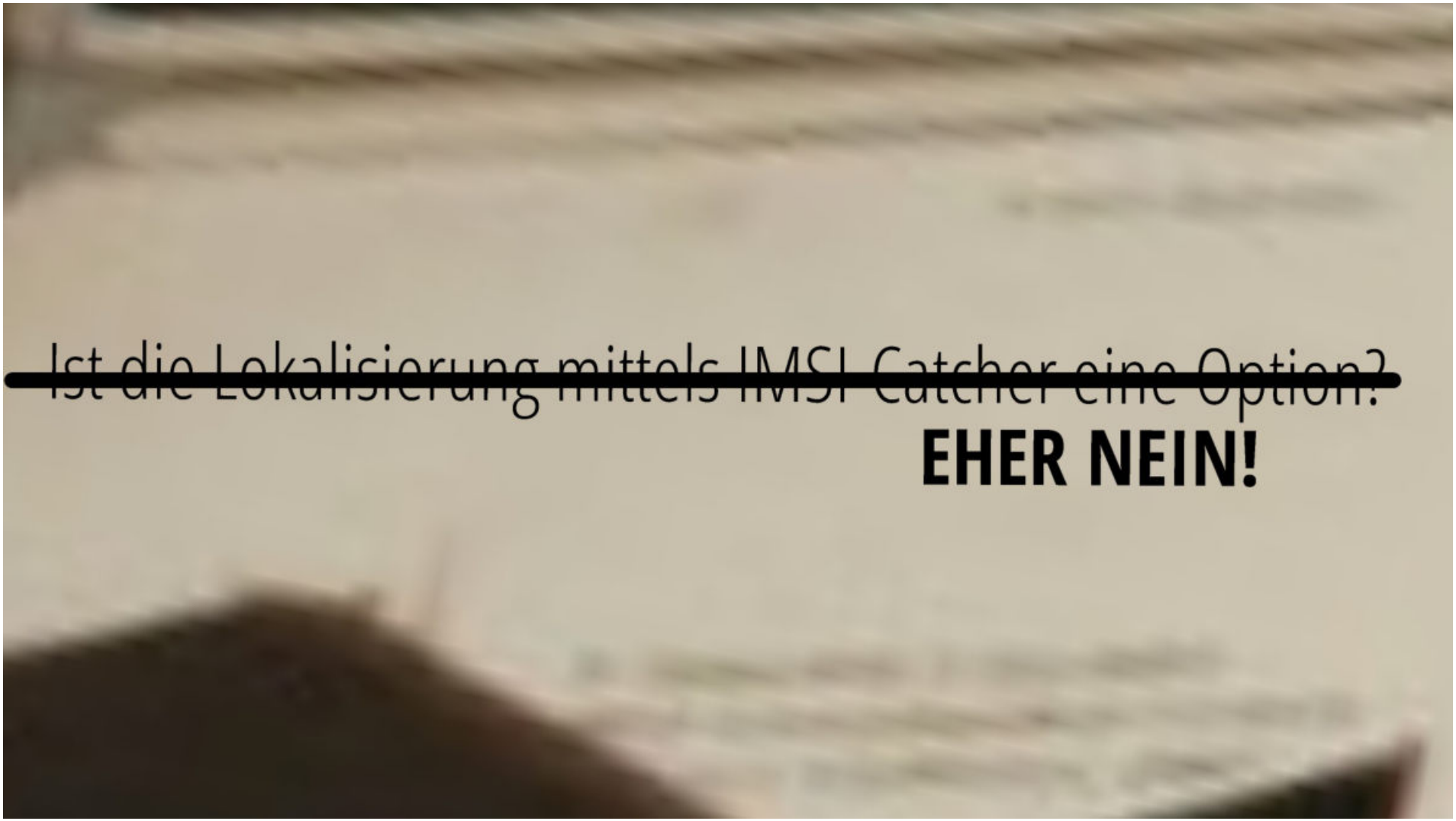
HöMS
HESSISCHE HOCHSCHULE FÜR ÖFFENTLICHES MANAGEMENT UND SICHERHEIT
University of Applied Sciences

- **Technische Funktion**
  - Simuliert gegenüber den Mobilfunk-teilnehmern eine Basisstation und gegenüber dem Mobilfunknetz einen Teilnehmer
- ***Nutzen:***
  - Lokalisierung von Mobilfunkteilnehmern
  - Abhören von Kommunikation

Cell Site Simulator
IMSI-Catcher

HöMS
HESSISCHE HOCHSCHULE FÜR ÖFFENTLICHES MANAGEMENT UND SICHERHEIT
University of Applied Sciences

- **Nachteile**
  - signifikanter Eingriff in ein öffentliches Kommunikationsnetz
  - hohe rechtliche Hürden für den Einsatz
  - Auflösung für Lokalisierung innerhalb eines Gebäudes zu grob
  - hohe Kosten, daher nur wenige Geräte im Einsatz
  - u.U. zu lange Vorlaufzeit, z.B. bei Gefahr im Verzug (Vermisstenfälle, Suizidgefahr, etc.)


~~Ist die Lokalisierung mittels IMSI Catcher eine Option?~~
EHER NEIN!


HöMS
HESSISCHE HOCHSCHULE FÜR ÖFFENTLICHES MANAGEMENT UND SICHERHEIT
University of Applied Sciences

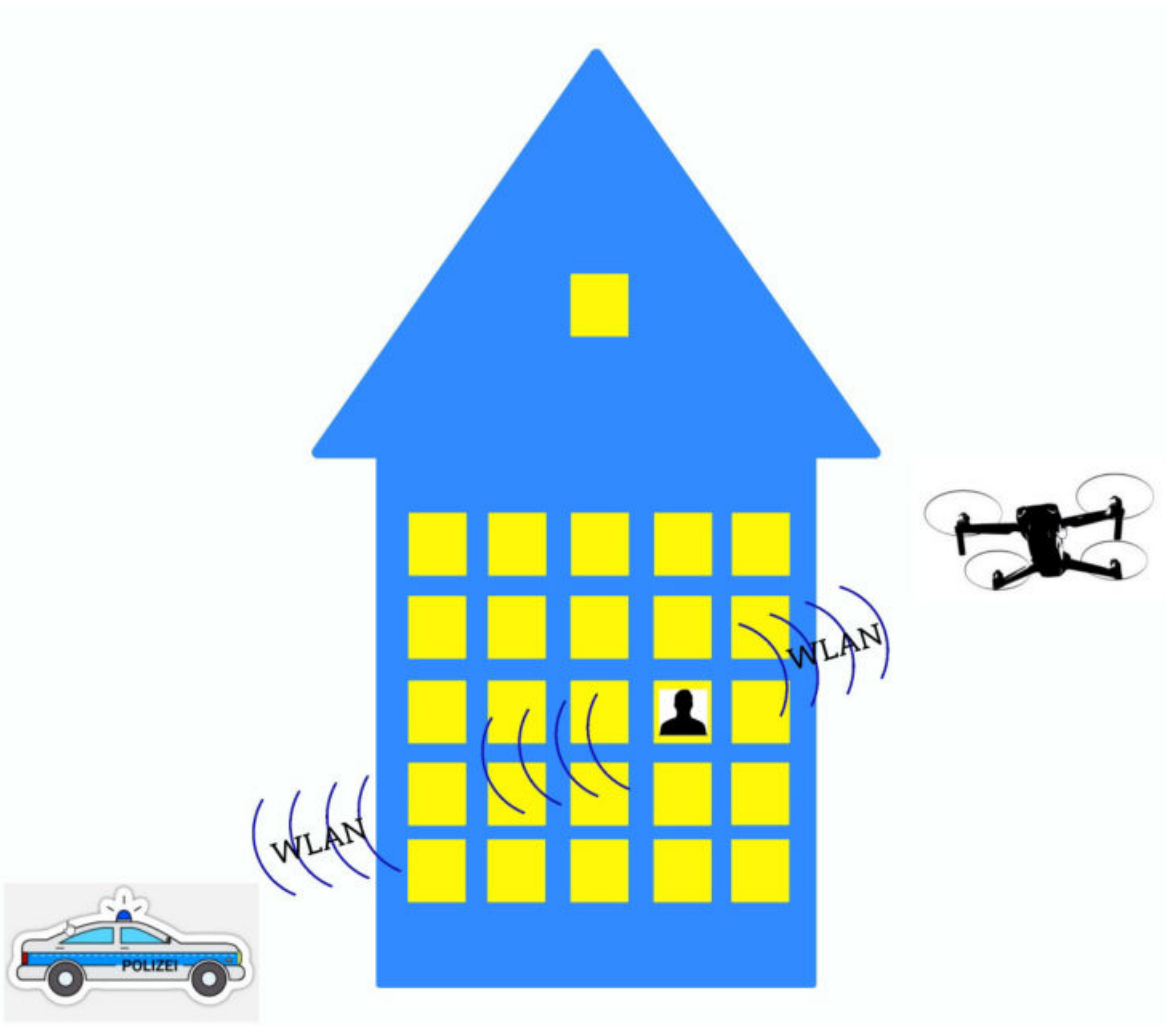

Blatt der coolen Ideen

Entwicklung eines "WLAN-OSI-2-Catchers"

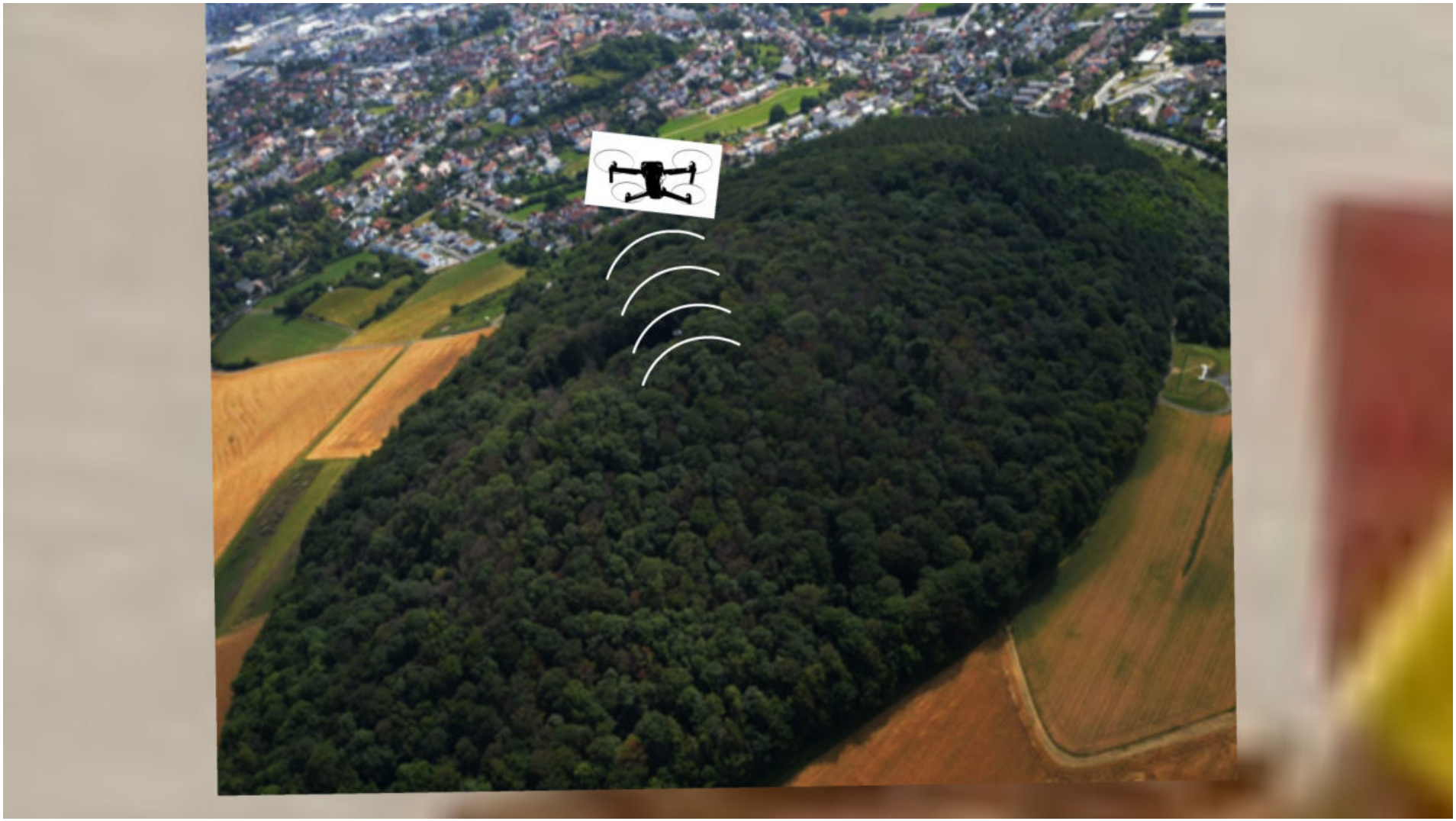
...nicht OSSI-Catcher

...nicht ~~OSSI-Catcher~~

...sondern OSI-2-Catcher!
Bezieht sich auf die 2. Schicht des
Open System Interconnection-Models

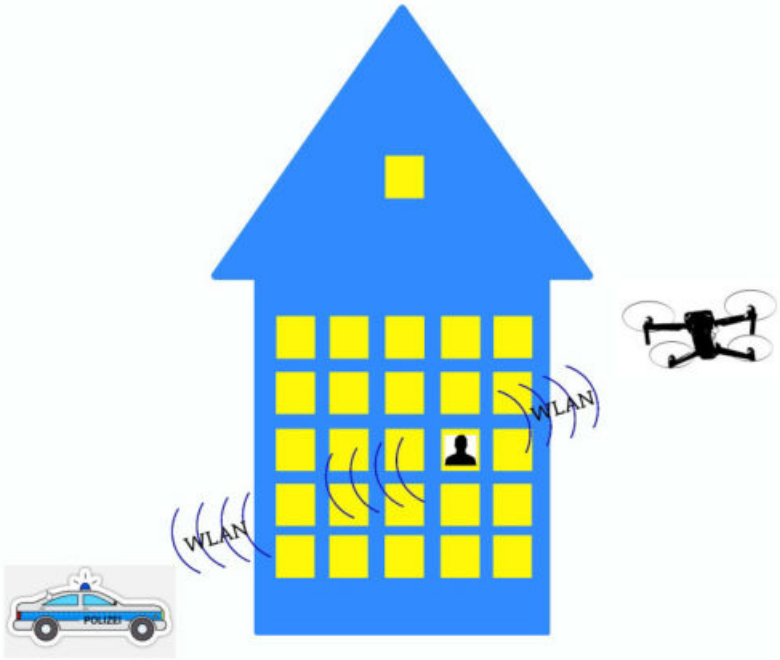

WLAN
WLAN
POLIZEI


The African Communist
HöMS
Der Präsident
DYRNOD BRANWEN
VOTA



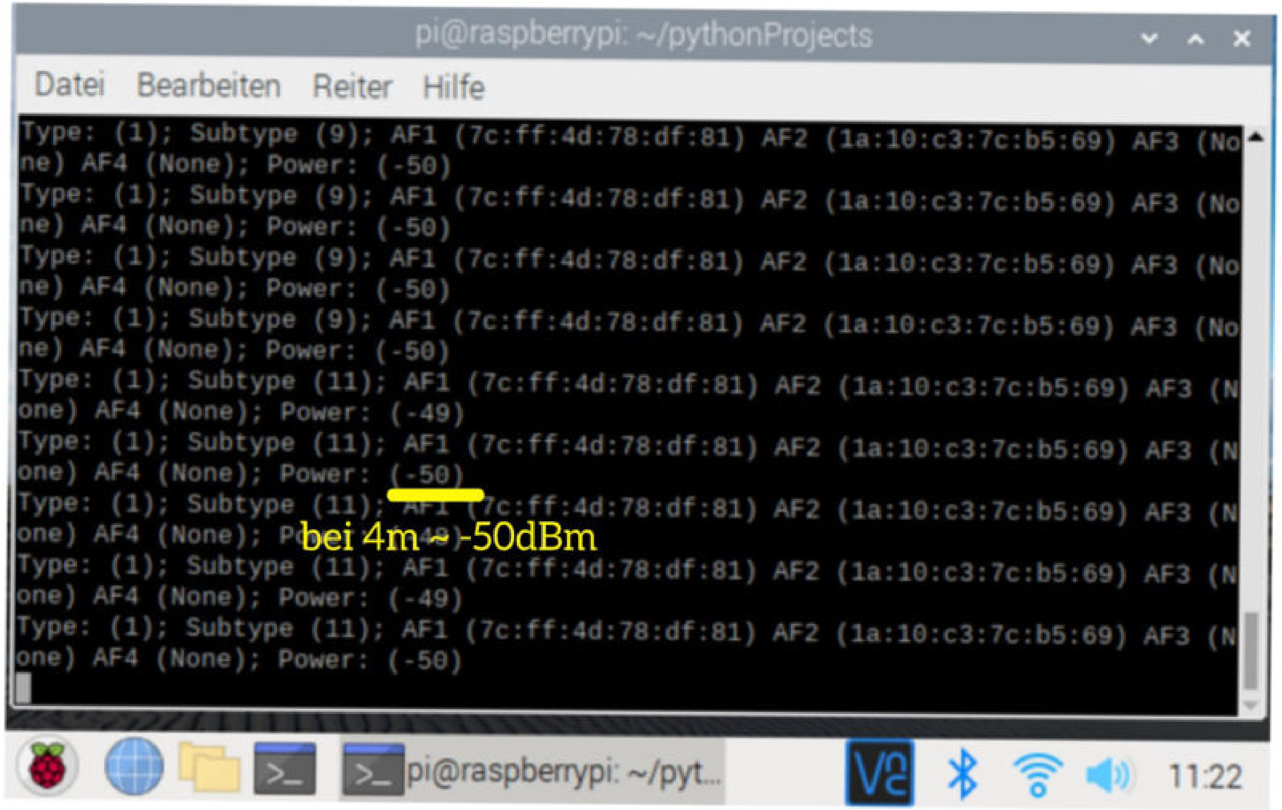
Blatt der coolen Ideen

Entwicklung eines
"WLAN-OSI-2-Catchers"

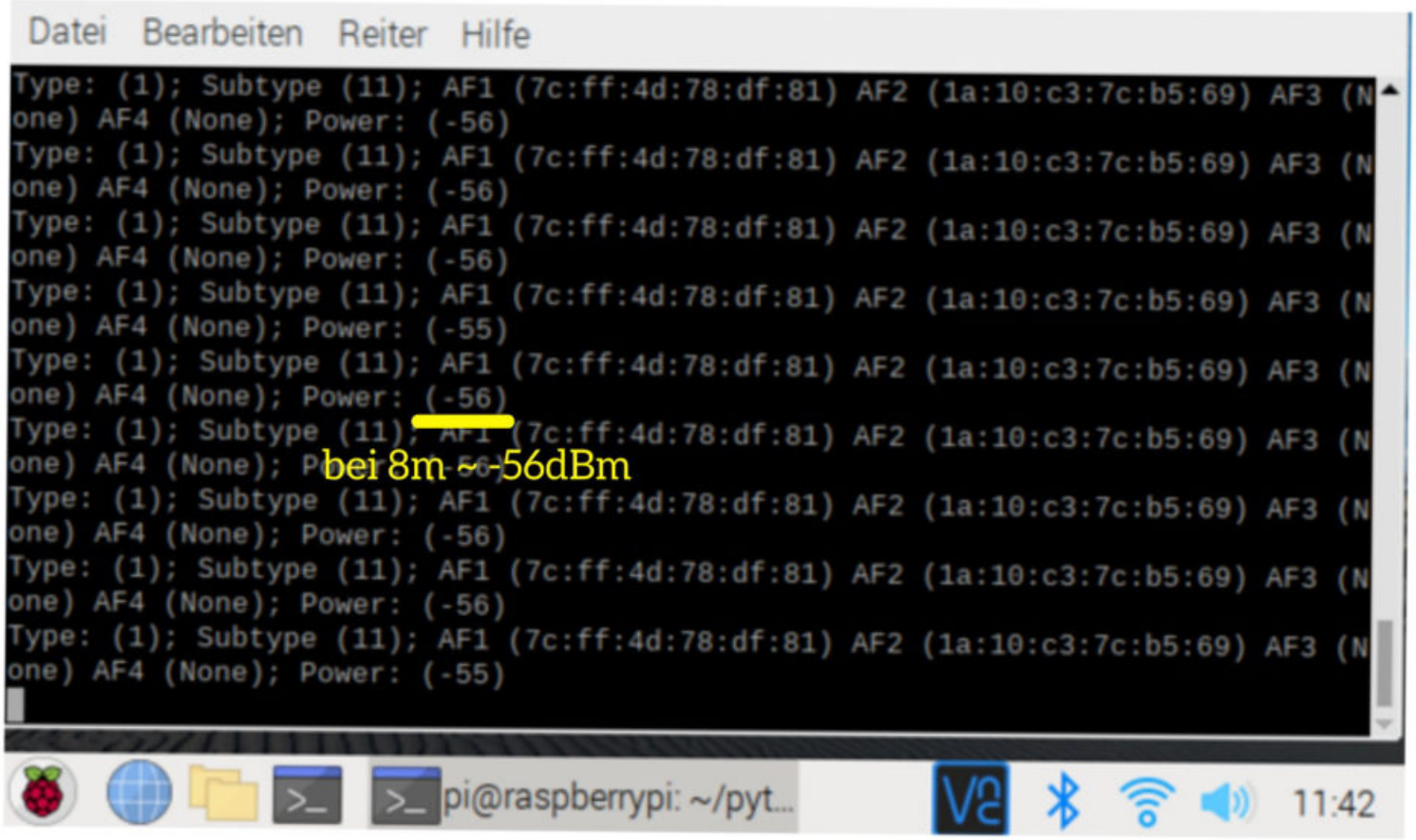


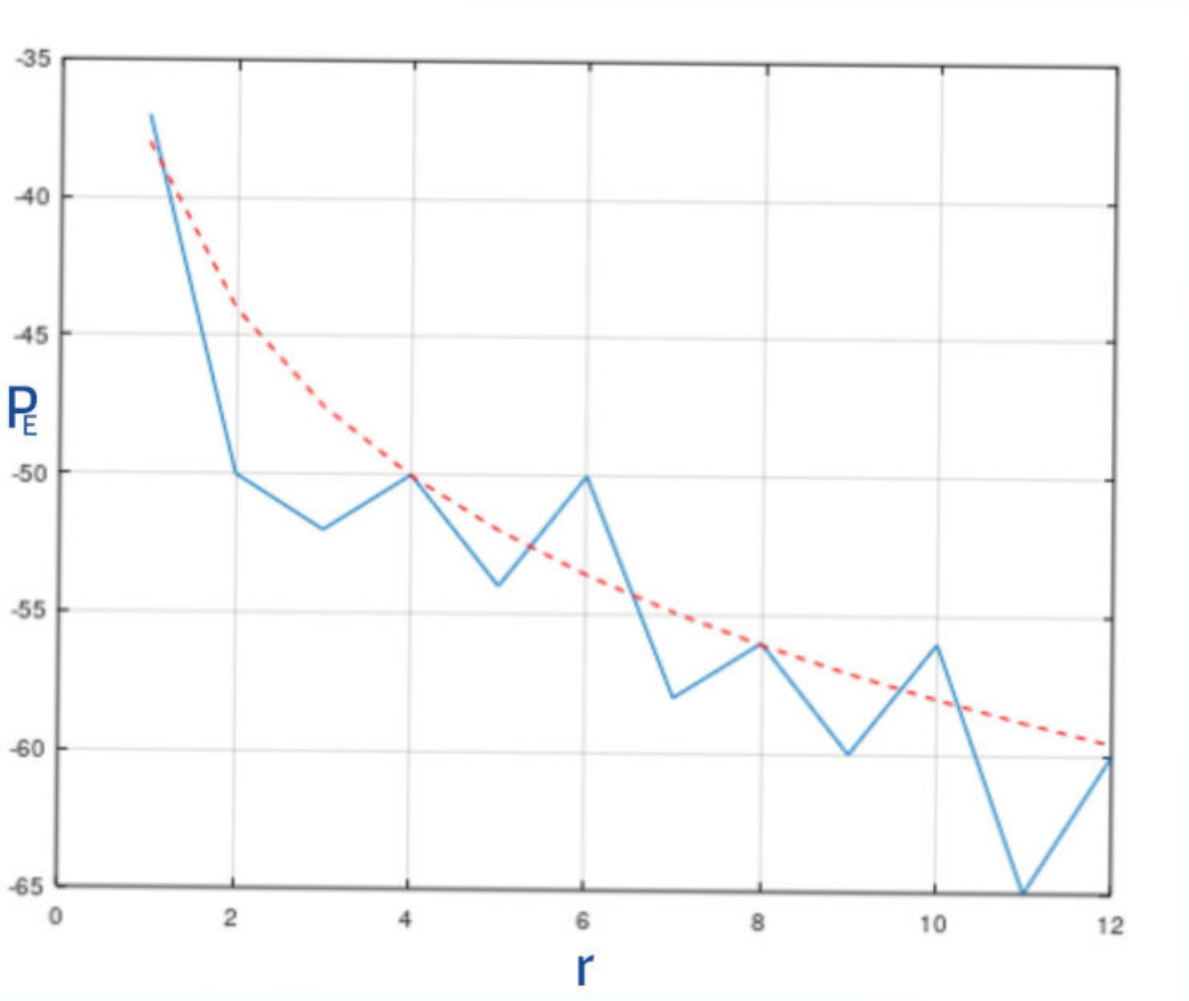
aufbauend auf Protocol-Analyzer aus Vorgängerprojekt zum Wiedererkennen von WLAN-Teilnehmern

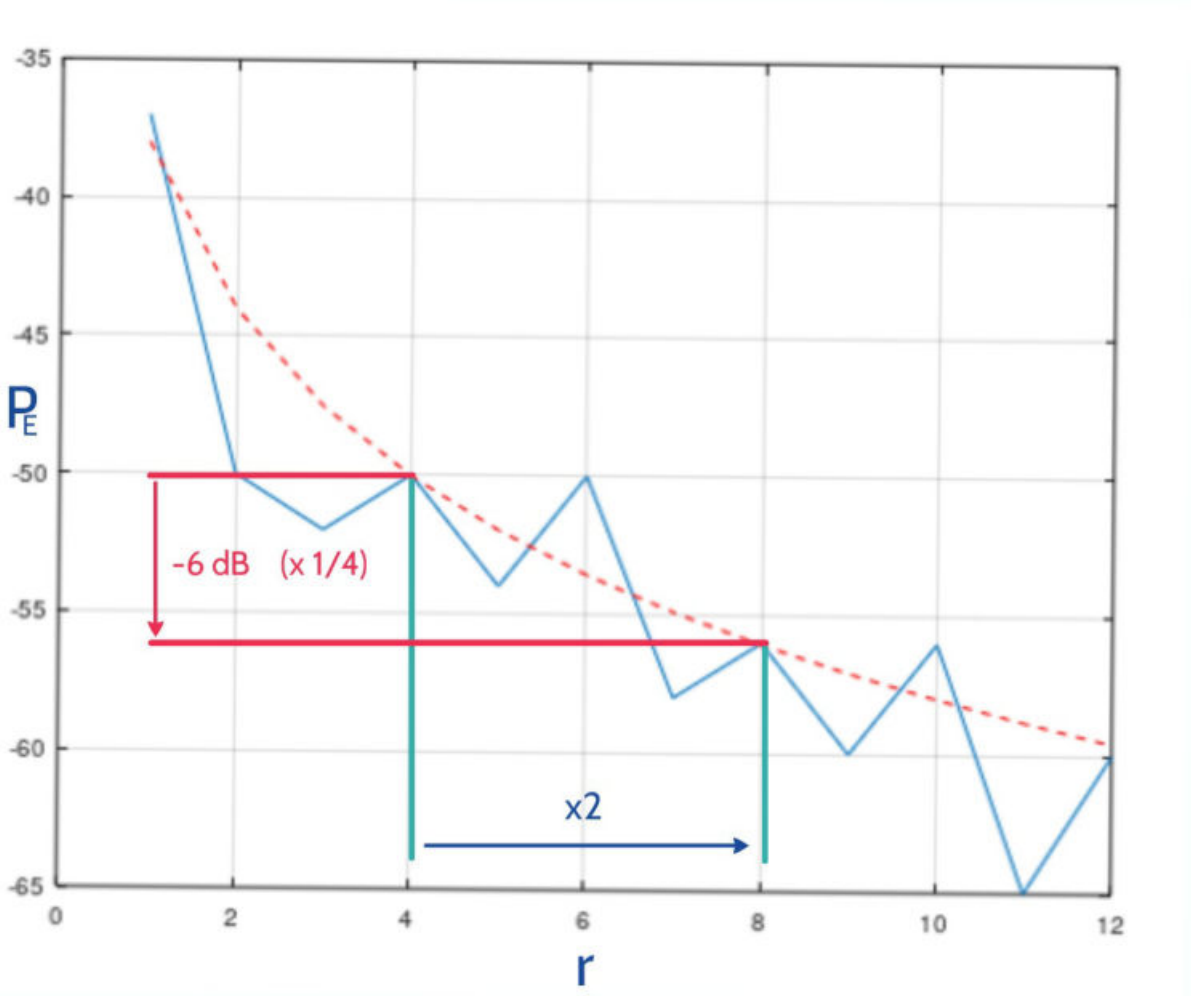
d = 4m;   L=--50 dBm


pi@raspberrypi: ~/pythonProjects
Datei Bearbeiten Reiter Hilfe
Type: (1); Subtype (9); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
Type: (1); Subtype (9); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
Type: (1); Subtype (9); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
Type: (1); Subtype (9); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-49)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
bei 4m ~ -50dBm
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-49)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-50)
pi@raspberrypi: ~/pyt...
11:22

d = 8m; L=-- 56 dBm


Datei Bearbeiten Reiter Hilfe
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-55)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-56)
Type: (1); Subtype (11); AF1 (7c:ff:4d:78:df:81) AF2 (1a:10:c3:7c:b5:69) AF3 (None) AF4 (None); Power: (-55)
bei 8m ~-56dBm
pi@raspberrypi: ~/pyt...
11:42


-35
-40
-45
-50
-55
-60
-65
P_E
0
2
4
6
8
10
12
r


-35
-40
-45
-50
-55
-60
-65
P_E
-6 dB (x 1/4)
x2
0
2
4
6
8
10
12
r

wo kommt das her?

Freiraumausbreitung

Schlaumeier-Blatt

Ausbreitungsmodell und unbekannte Sendeleistung

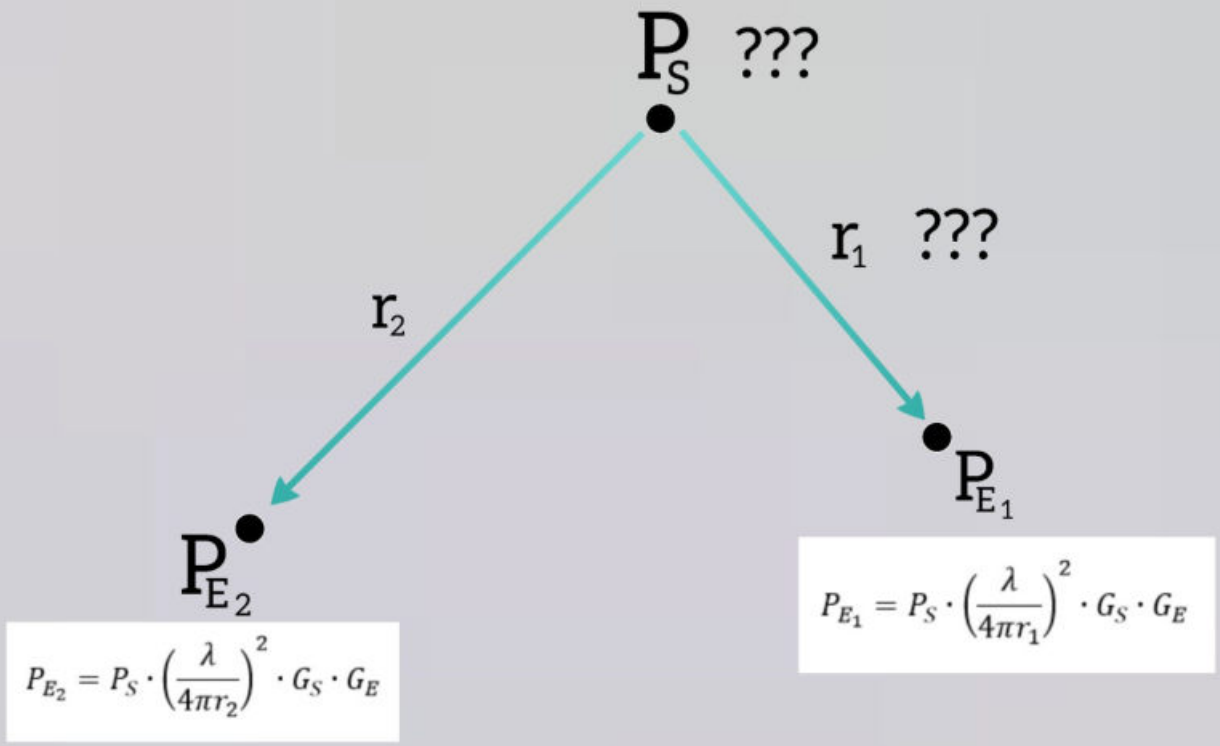
Freiraumausbreitung

Distanzermittlung via Feldmessung

Freiraumausbreitung

$$P_E = P_S \cdot \left(\frac{\lambda}{4\pi r}\right)^2 \cdot G_S \cdot G_E$$

Distanzermittlung via Feldmessung

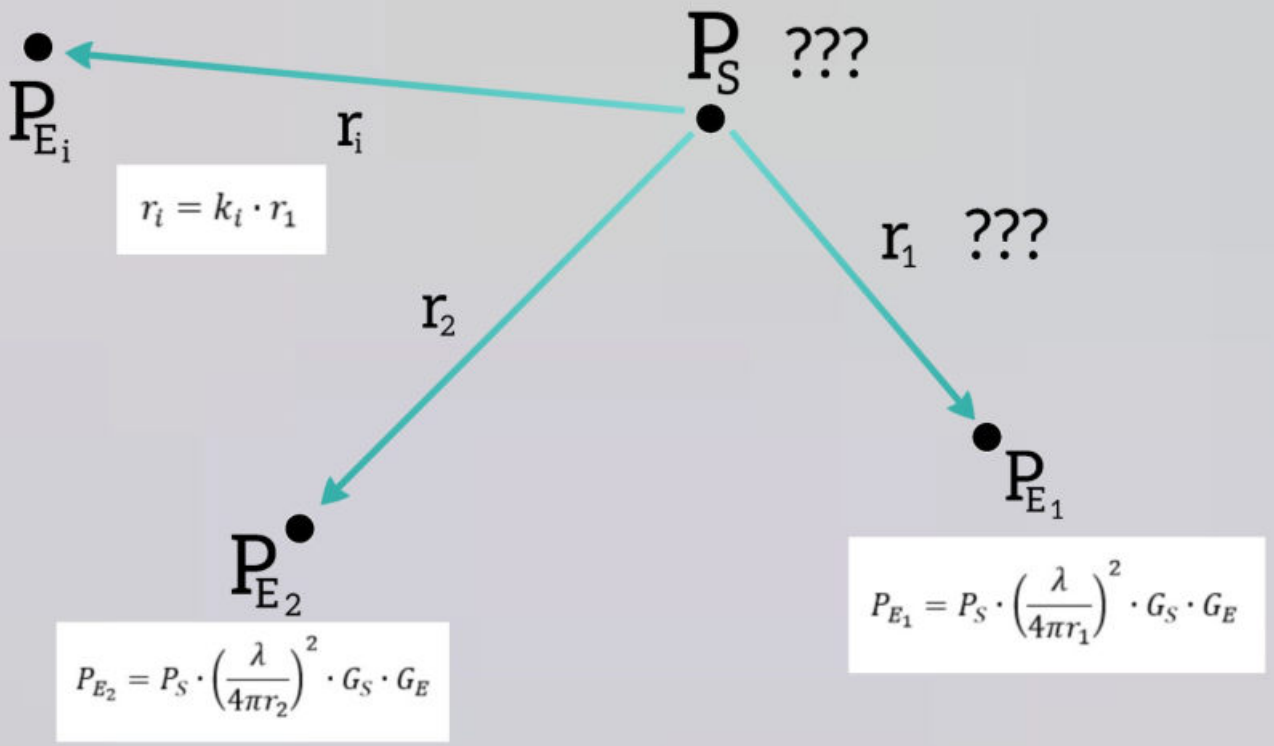


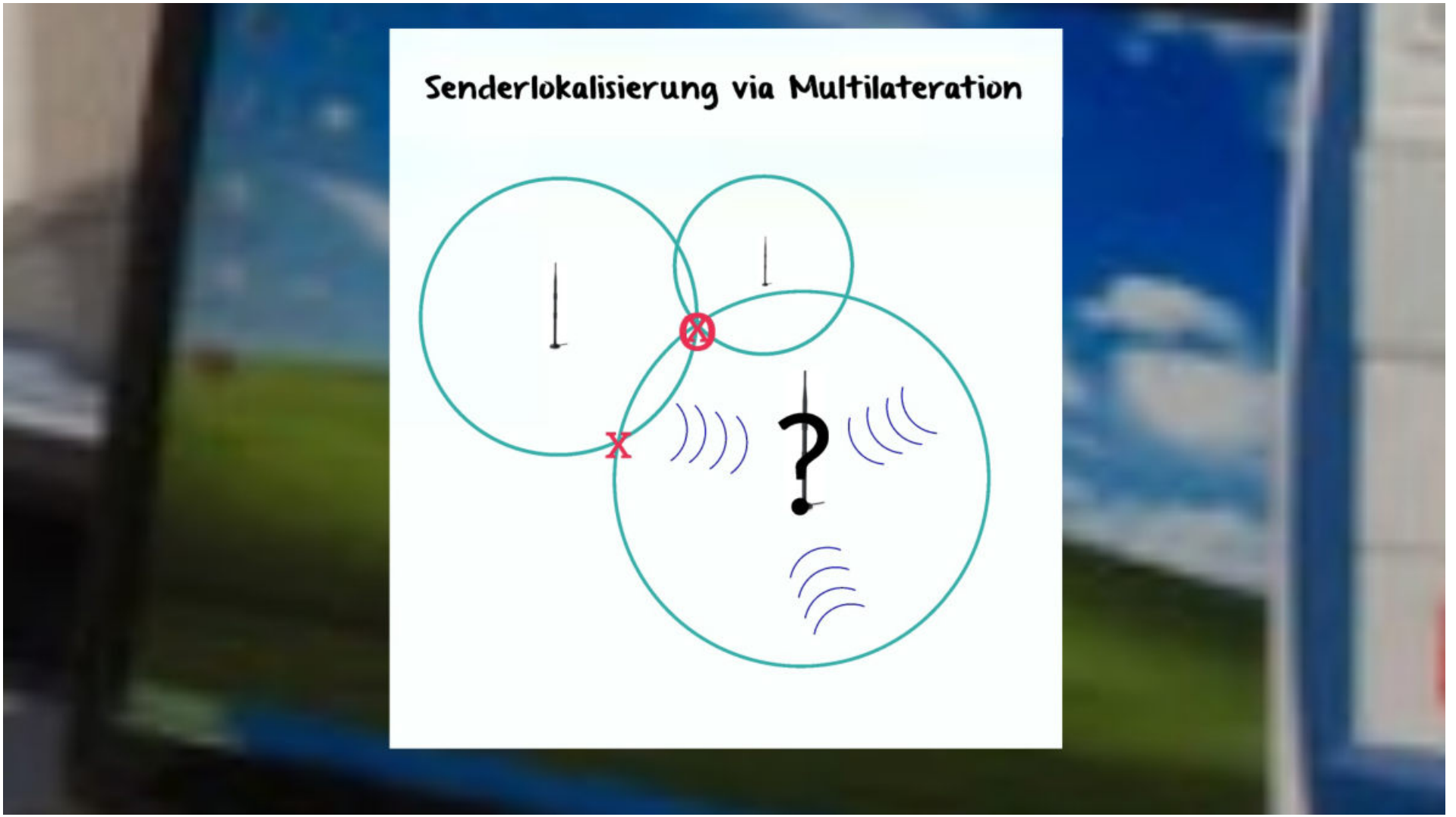
$$\frac{P_{E_2}}{P_{E_1}} = \frac{r_1^2}{r_2^2}$$

$$r_i = k_i \cdot r_1$$

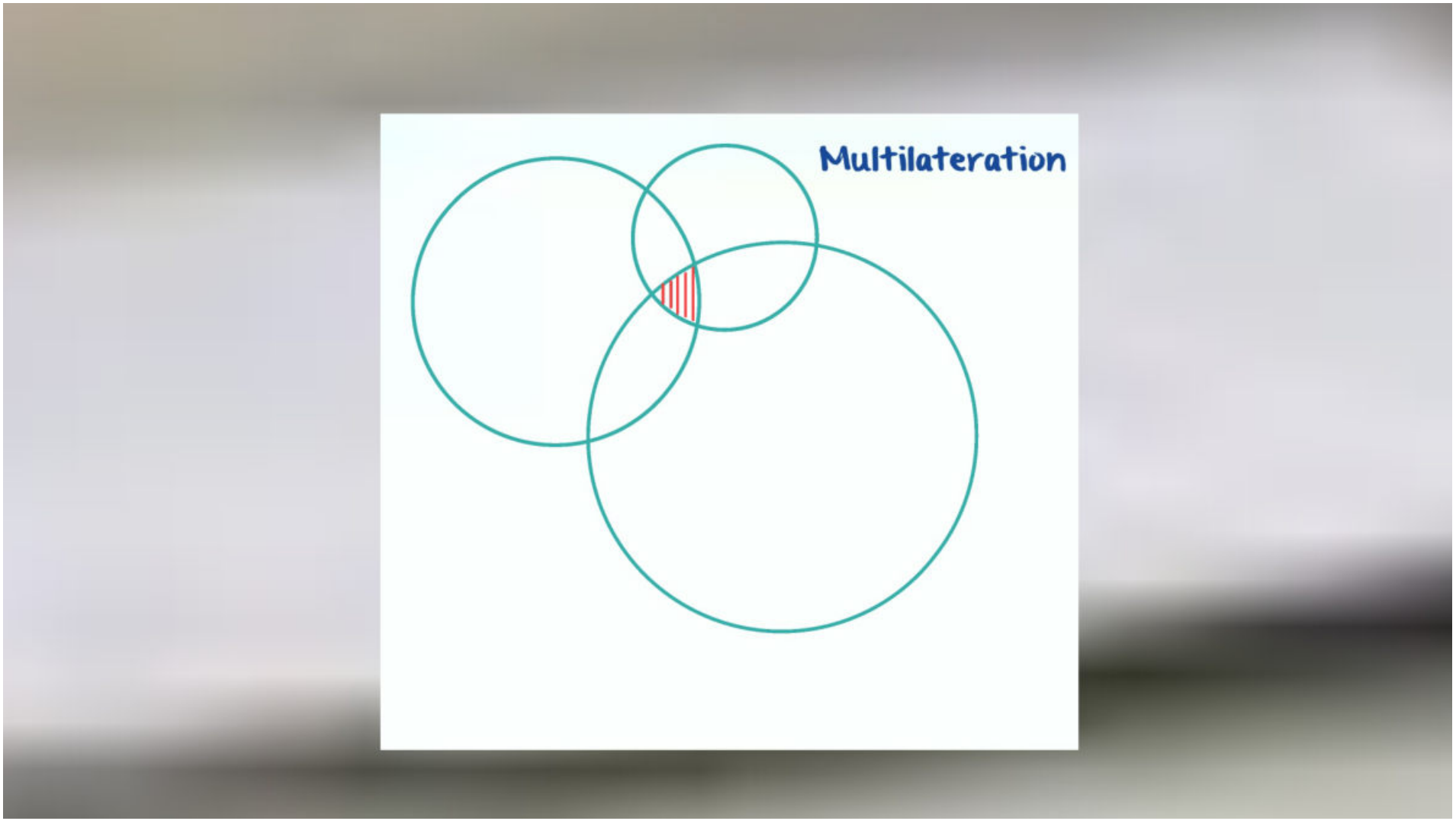
$$k_i = \sqrt{\frac{P_{E_1}}{P_{E_i}}}$$

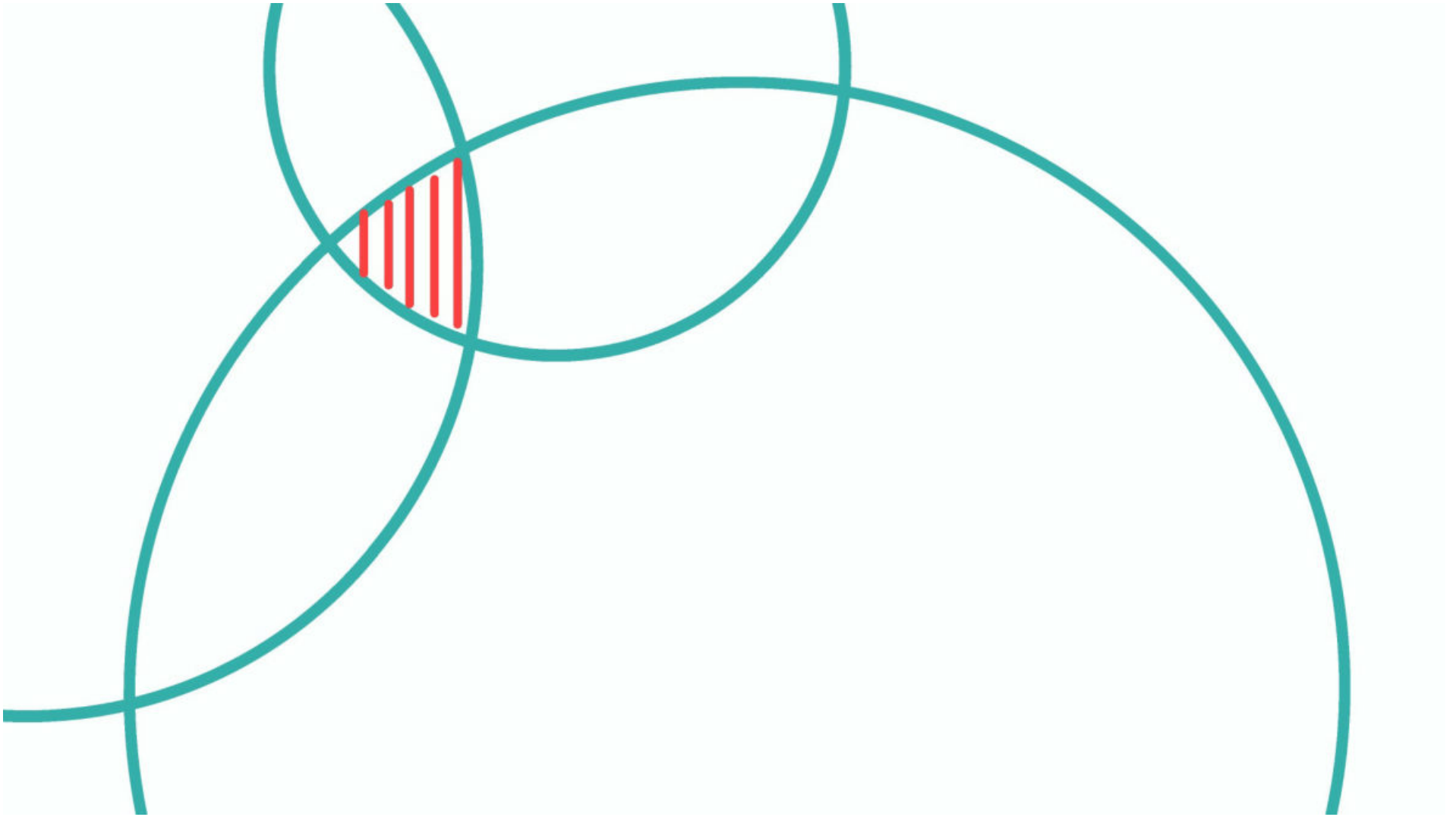
Distanzermittlung via Feldmessung

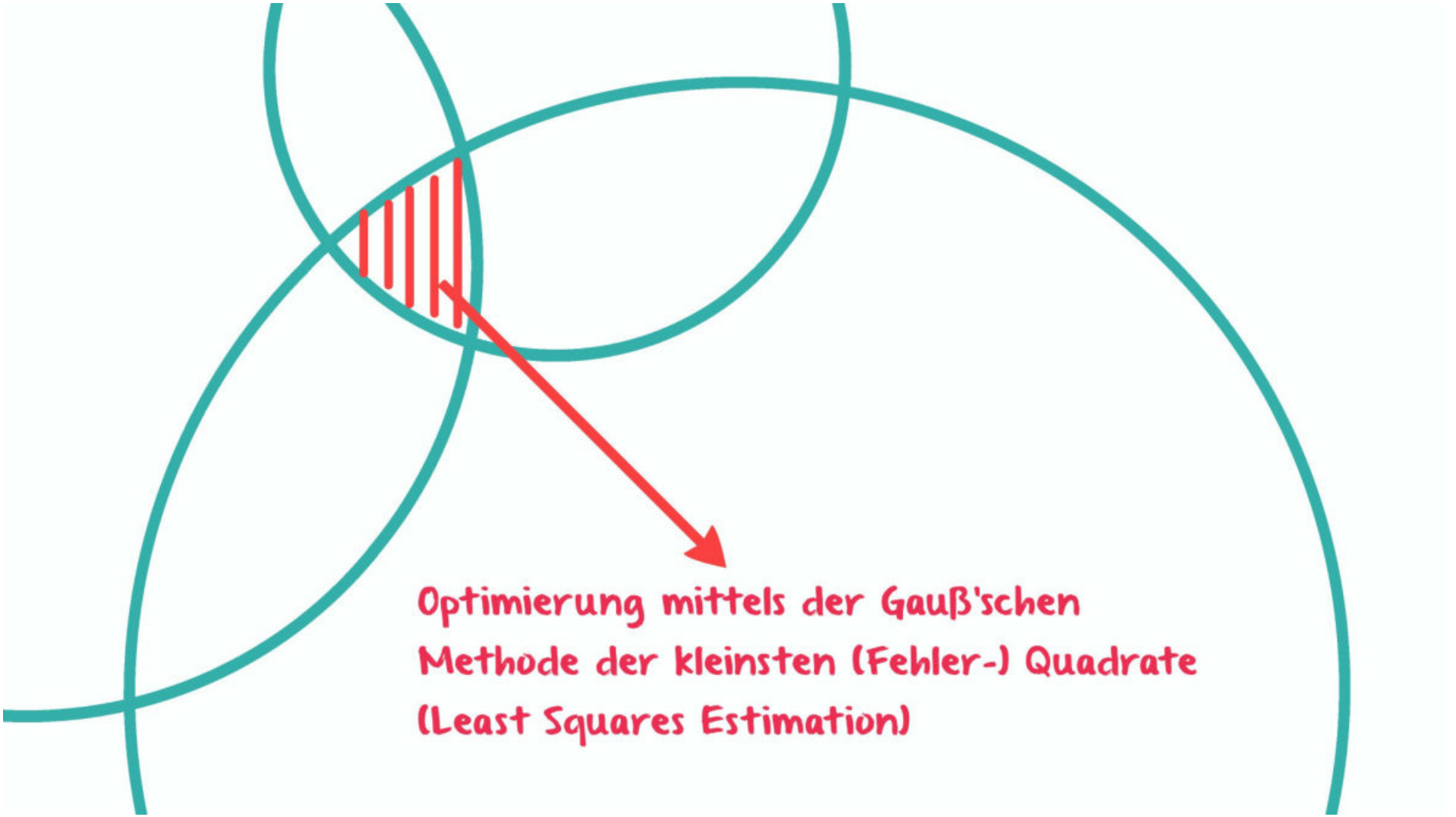



Senderlokalisierung via Multilateration
X
?


HöMS


Multilateration




Optimierung mittels der Gauß'schen
Methode der kleinsten (Fehler-) Quadrate
(Least Squares Estimation)

2D: 2 gesuchte Unbekannte: x0, y0

2 weitere Unbekannte: w0 (Linearisierung), r1 (Sendeleistung unbekannt)

=> min. 4 Messungen!!!

3D: 3 gesuchte Unbekannte: x0, y0, z0

2 weitere Unbekannte: w0 (Linearisierung), r1 (Sendeleistung unbekannt)

=> min. 5 Messungen!!!

$$\sum_{i=1}^{n} \begin{pmatrix} 2x_i^2 & 2x_iy_i & 2x_iz_i & -x_i & x_ik_i^2 \\ 2x_iy_i & 2y_i^2 & 2y_iz_i & -y_i & y_ik_i^2 \\ 2x_iz_i & 2y_iz_i & 2z_i^2 & -z_i & z_ik_i^2 \\ -2x_i & -2y_i & -2z_i & 1 & -k_i^2 \\ 2x_ik_i^2 & 2y_ik_i^2 & 2z_ik_i^2 & -k_i^2 & k_i^4 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{x_0} \\ \boldsymbol{y_0} \\ \boldsymbol{z_0} \\ \boldsymbol{w_0} \\ \boldsymbol{p_1} \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} x_iK_i \\ y_iK_i \\ z_iK_i \\ -K_i \\ k_i^2K_i \end{pmatrix}$$

$$\sum_{i=1}^{n} \begin{pmatrix} 2x_i^2 & 2x_iy_i & 2x_iz_i & -x_i & x_ik_i^2 \\ 2x_iy_i & 2y_i^2 & 2y_iz_i & -y_i & y_ik_i^2 \\ 2x_iz_i & 2y_iz_i & 2z_i^2 & -z_i & z_ik_i^2 \\ -2x_i & -2y_i & -2z_i & 1 & -k_i^2 \\ 2x_ik_i^2 & 2y_ik_i^2 & 2z_ik_i^2 & -k_i^2 & k_i^4 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{x_0} \\ \boldsymbol{y_0} \\ \boldsymbol{z_0} \\ \boldsymbol{w_0} \\ \boldsymbol{p_1} \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} x_iK_i \\ y_iK_i \\ z_iK_i \\ -K_i \\ k_i^2K_i \end{pmatrix}$$

Lösung von x0, y0, z0 via Gauß-Elimination,
...kann heute jeder bessere Taschenrechner!

Simulation

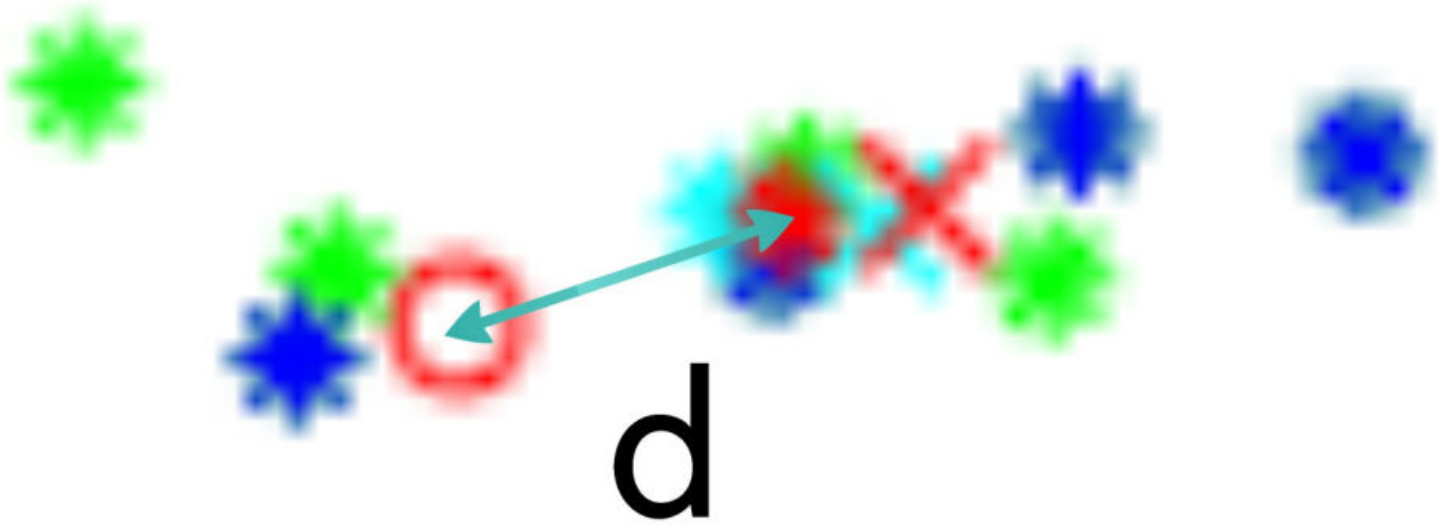
Fehlerbeaufschlagung

wegen des zu erwartenden
Messfehlers bei der Distanzmessung

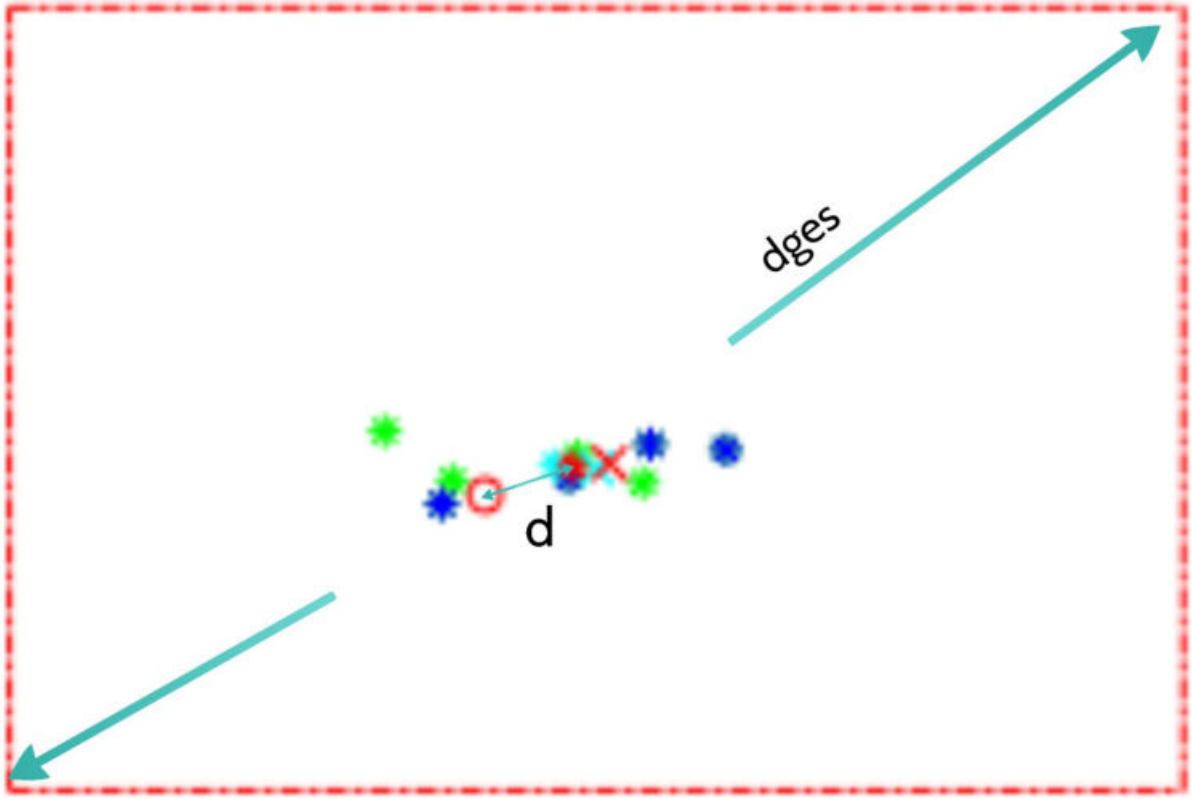
aufgrund von systemischen
Messfehlern und unterschiedlichen
Materialeigenschaften

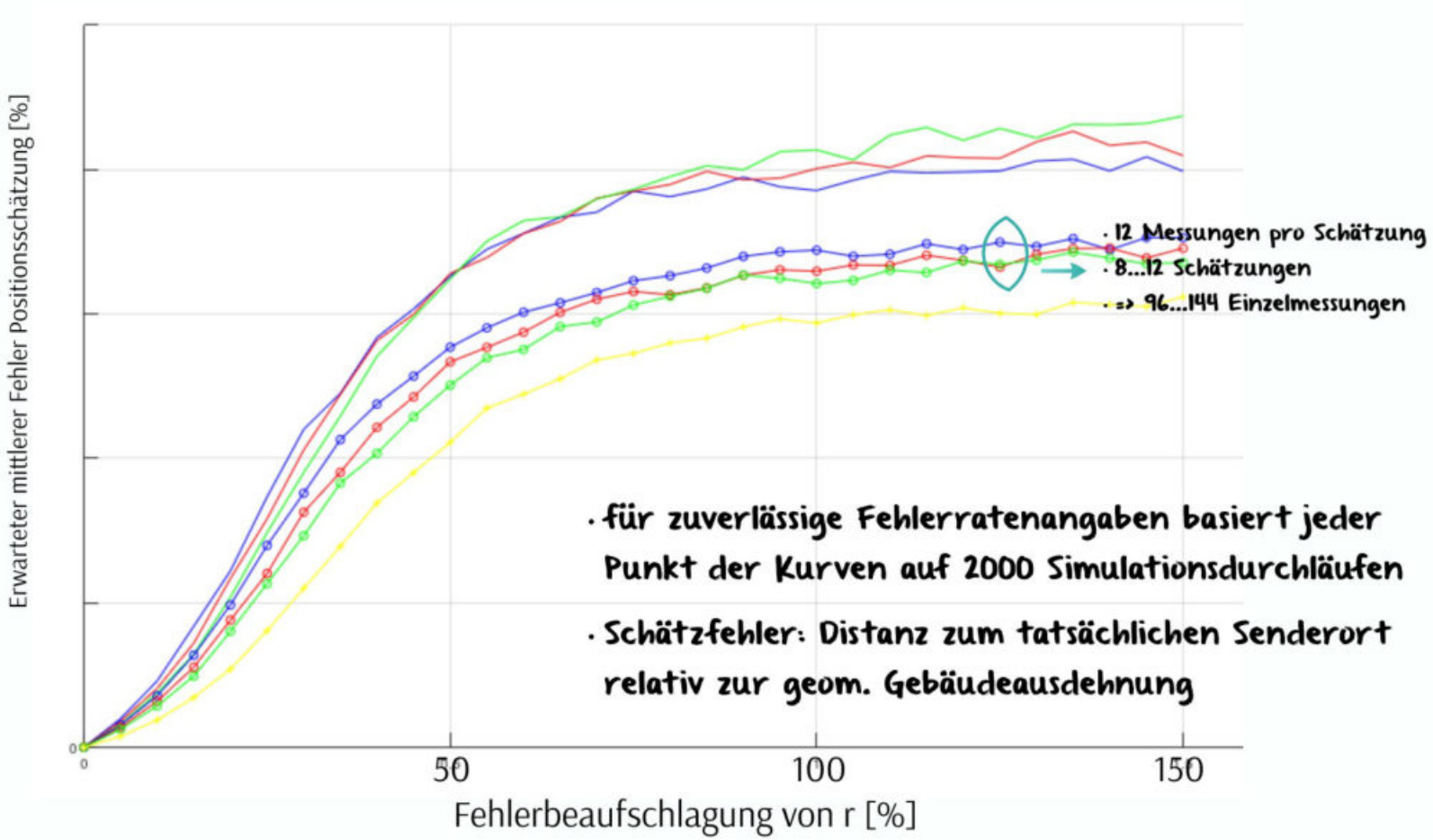
$$r' = r * (1 + \text{Fehlerrate}[\%] * \text{Normalverteilung})$$

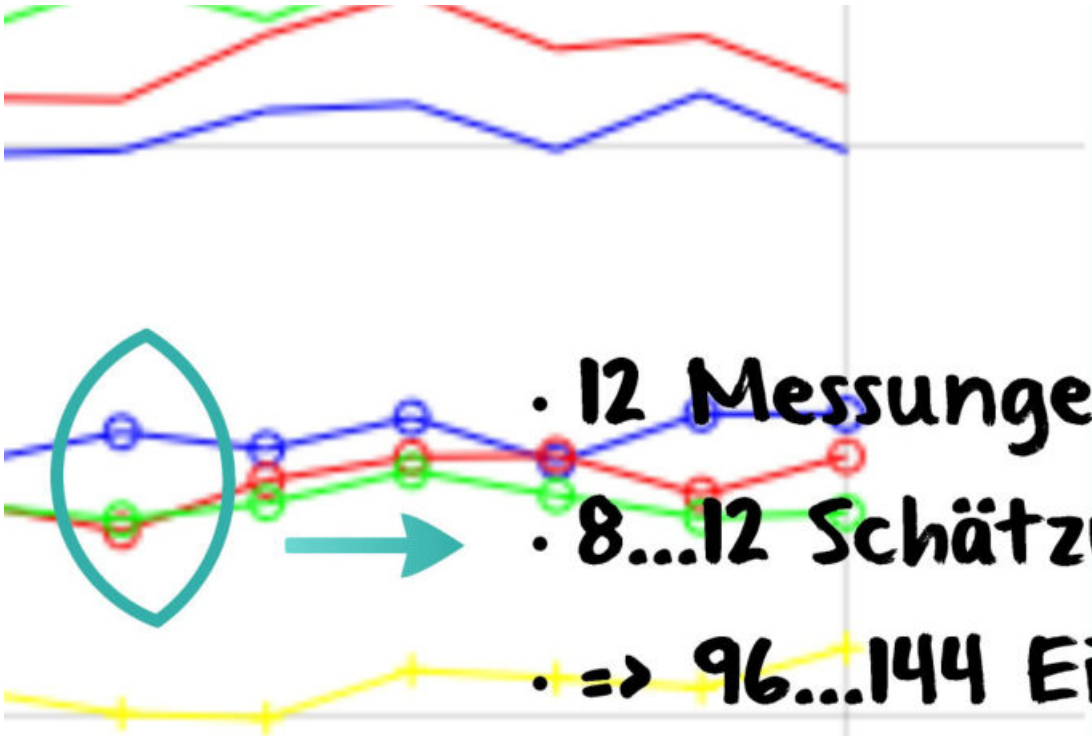
Fehler-Maß zur Schätzgüte


d

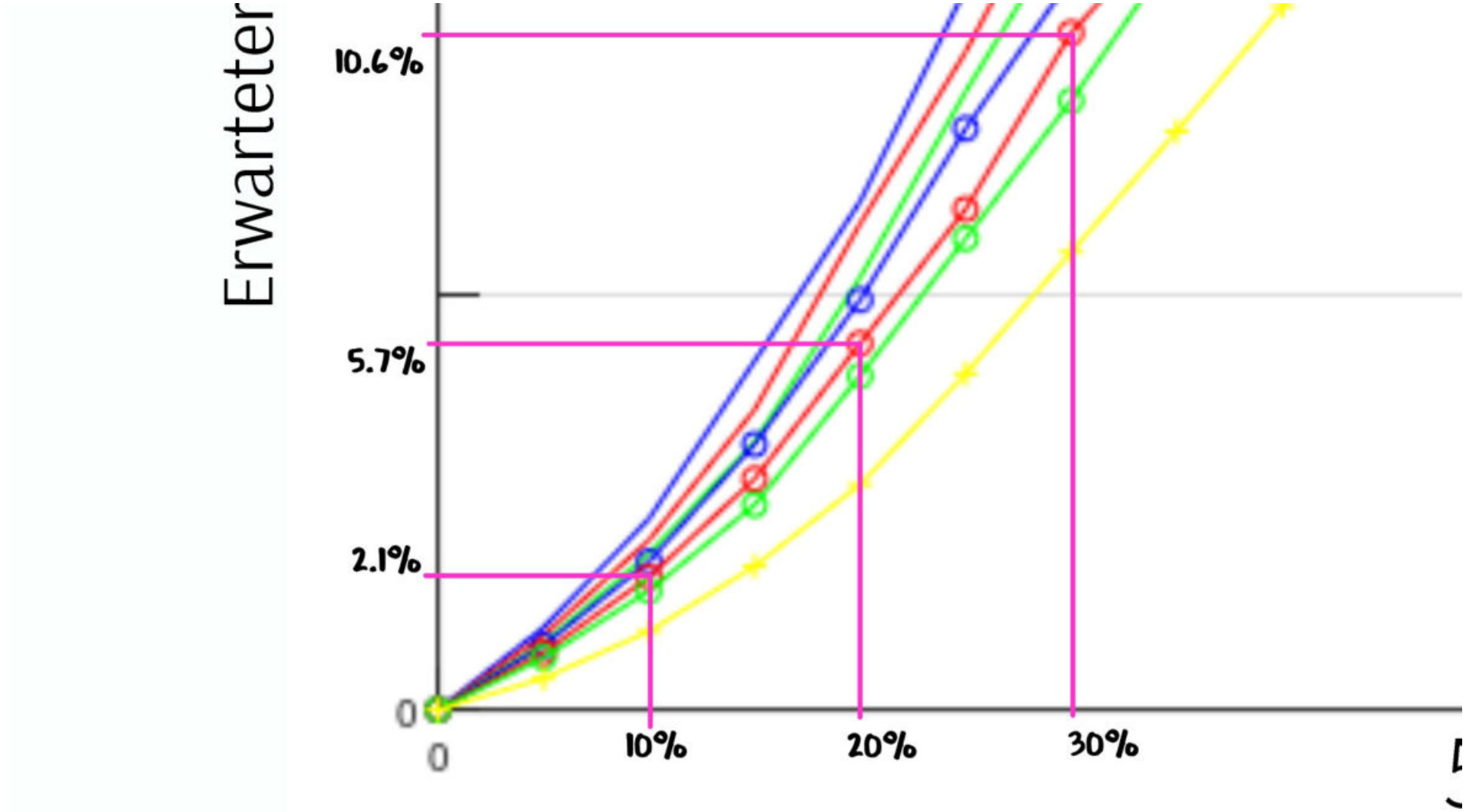
Fehler-Maß zur Schätzgüte




Erwarteter mittlerer Fehler Positionsschätzung [%]
0
50
100
150
Fehlerbeaufschlagung von r [%]
· 12 Messungen pro Schätzung
· 8...12 Schätzungen
· => 96...144 Einzelmessungen
· für zuverlässige Fehlerratenangaben basiert jeder Punkt der Kurven auf 2000 Simulationsdurchläufen
· Schätzfehler: Distanz zum tatsächlichen Senderort relativ zur geom. Gebäudeausdehnung



- 12 Messungen pro Schätzung
- 8...12 Schätzungen
- => 96...144 Einzelmessungen


Erwarteter
10.6%
5.7%
2.1%
0
0
10%
20%
30%

WLAN-OSI-2-Catcher

HöMS
HESSISCHE HOCHSCHULE FÜR ÖFFENTLICHES MANAGEMENT UND SICHERHEIT
University of Applied Sciences

- **Zusammenfassung**
  - geringfügiger bis kein Eingriff in öffentliche Kommunikationsnetze
  - keine aufwendige Hardware
    - keine hohe Rechenleistung und lediglich omnidirektionale Antenne für Multilateration erf.
  - geringe Kosten
    - ... daher prinzipiell in großer Anzahl beschaffbar
    - ... daher geringe Vorlaufzeit , z.B. bei Gefahr im Verzug (Vermisstenfälle, Suizidgefahr, etc.)
  - geringes Gewicht (~ 300g)
    - ... daher portable, mobile und drohnen-gestützte Anwendung möglich

Das Cyber Stilzchen meint...

- WLAN-Messungen leicht durchführbar
- Lokalisierungs-Schätzverfahren funktioniert
- Fehler beherrschbar
- OSI-2-Catcher auf günstiger Hardware (Raspi) implementierbar

Das Cyber Stilzchen meint...

HöMS Cyber-Radio

- Heute back' ich...
  ... einen Algorithmus
- Morgen brau' ich...
  ... mir 'nen OSI-2-Catcher
- Übermorgen
  ... lokalisiere ich Vermisste
  und auch Gauner


HöMS
HESSISCHE HOCHSCHULE
FÜR ÖFFENTLICHES MANAGEMENT
UND SICHERHEIT
University of Applied Sciences


Fine
Prof. Dr.-Ing. Steffen Bug, HöMS