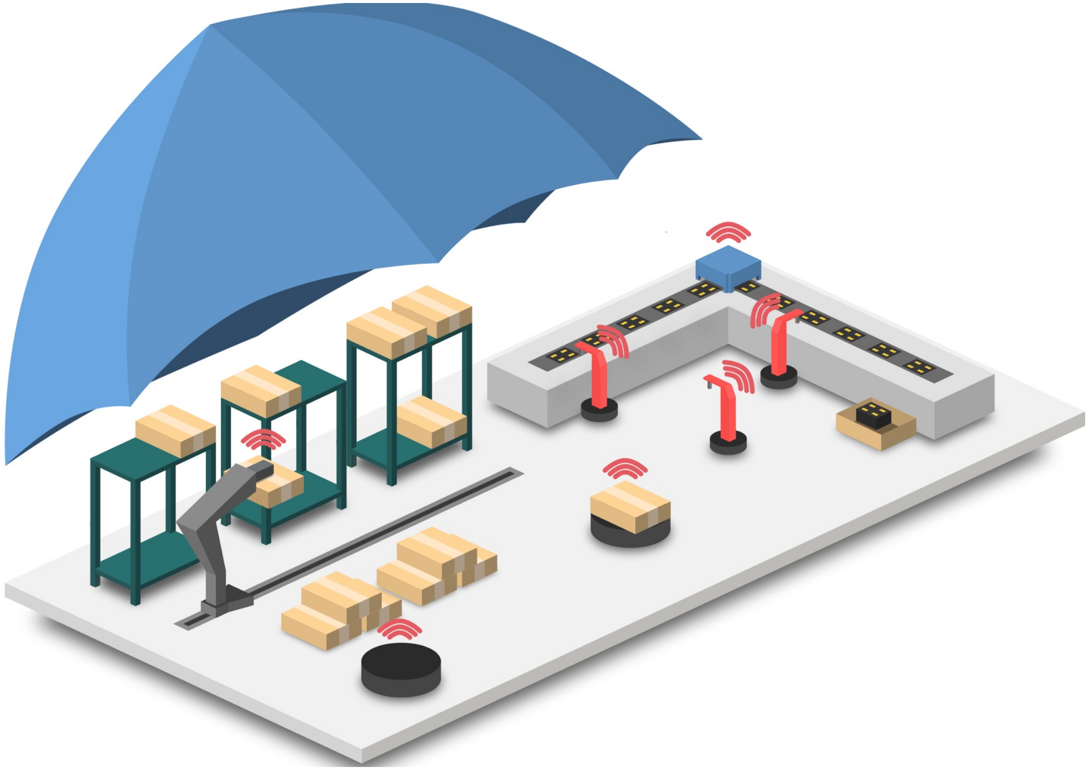
Scanner 1: A wireless shield for protecting private 5G networks



Stefan Valentin and Martin Stiemerling

da/net research group (h_da), Trailblazer Networks

5G Campus Networks: A German success story

- *5G Campus Network:* Local 5G network, operating license owned by private entity
- In Germany: Dedicated 3.7-3.8 GHz band since July 2019
- Since then: **~220 licenses granted [1]**
- Used: On industrial sites, on university and hospital campuses, by media outlets, ...
- New: Not driven by large operators but by small system houses and integrators

Problems: Security rather add-on than foundation, poor automation

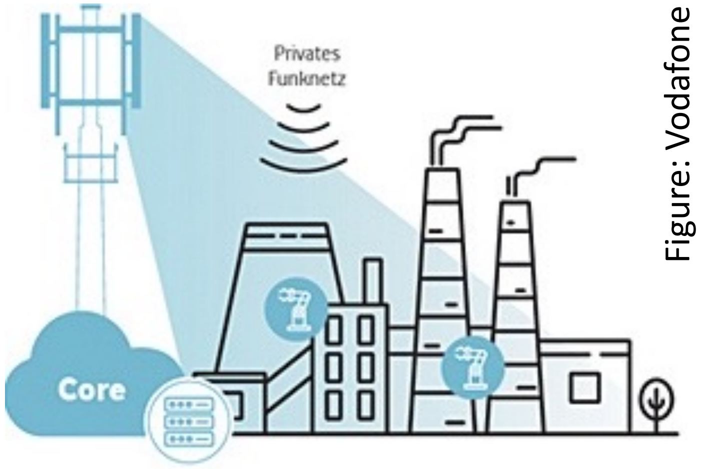


Figure: Vodafone

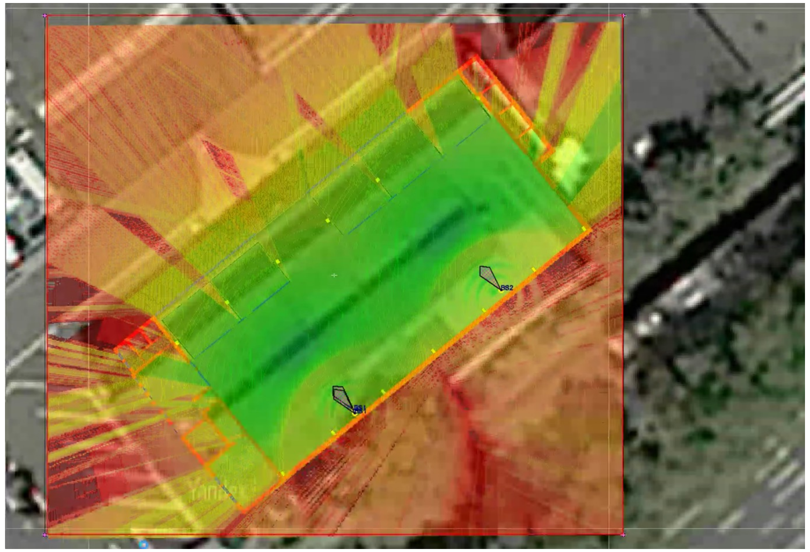


Figure: Valentin, Google

This talk…

…will introduce Scanner 1: A magical black box with antennas

Any questions? Bye! ☺

This talk…

…will introduce Scanner 1: A ~~magical black box with antennas~~ solution to *some* security and *some* automation problems of 5G Campus Networks

Lots of questions!

Outline

- Why we should not trust 5G!
- Scanner 1: A watchdog for 5G
  - Idea and method
  - Measurements
  - Automation
- Trailblazer Networks
- Summary and next steps

Would you realize, if your modem opens a covert channel to send your data to someone else?

Photo: dpa/Michael Kappeler/dpabil

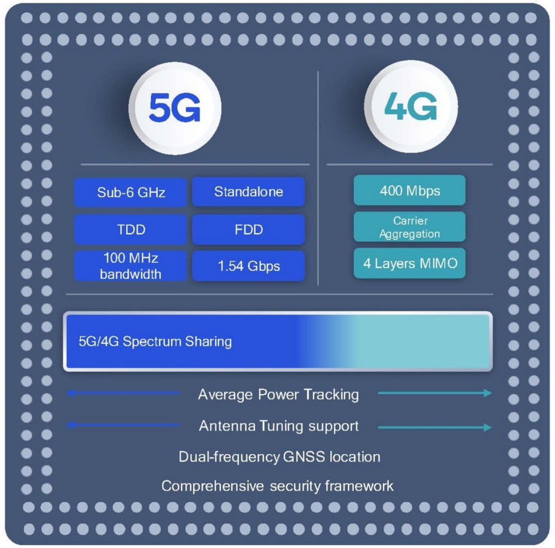
She didn’t! [2]

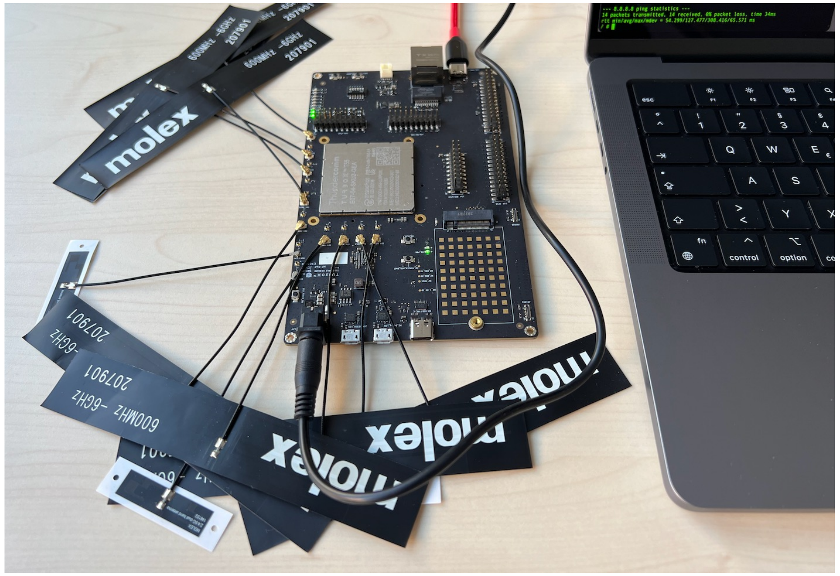
(and I wouldn’t)

Why we should **not** trust 5G!

- 5G modems are:
  - all designed and manufactured outside the EU
  - complex System-on-Chips (SoCs) with patchable microcode, multi-band, multi-standard
  - the ideal base for eavesdropping, man-in-the-middle attacks and covert channels
- 5G modems are a tempting target:
  - 1.2B 5G global subscribers [3]
  - 220+ industrial 5G networks in Germany
- **Consequence: Zero trust for 5G modems!**
- How to use such a modem without trust?
  => Add a watchdog!

Qualcomm's 315 IoT modem



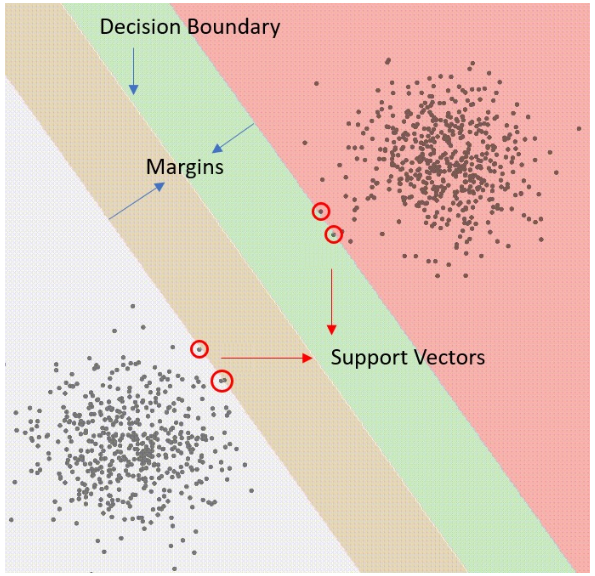


Thundercomm's T55G board with Qualcomm X55

A watchdog for 5G: Idea and method

- Use a radio scanner to detect rogue signals
  - Embed it into an 5G device to check on itself
- Scanner permanently observes the spectrum
  - Broadband: Sweep every ms
  - Narrowband: “Zoom in” if needed
- Basic method:
  - Compare operational vs. expected state
  - Classification based on
    - Signal processing (filtering, segmentation)
    - Machine Learning (ML): Supported Vector Machines (SVMs)
  - We call this method: *Spectral Intrusion Detection (SID)*

Inspiration: Whistler TRX-2 radio scanner and others

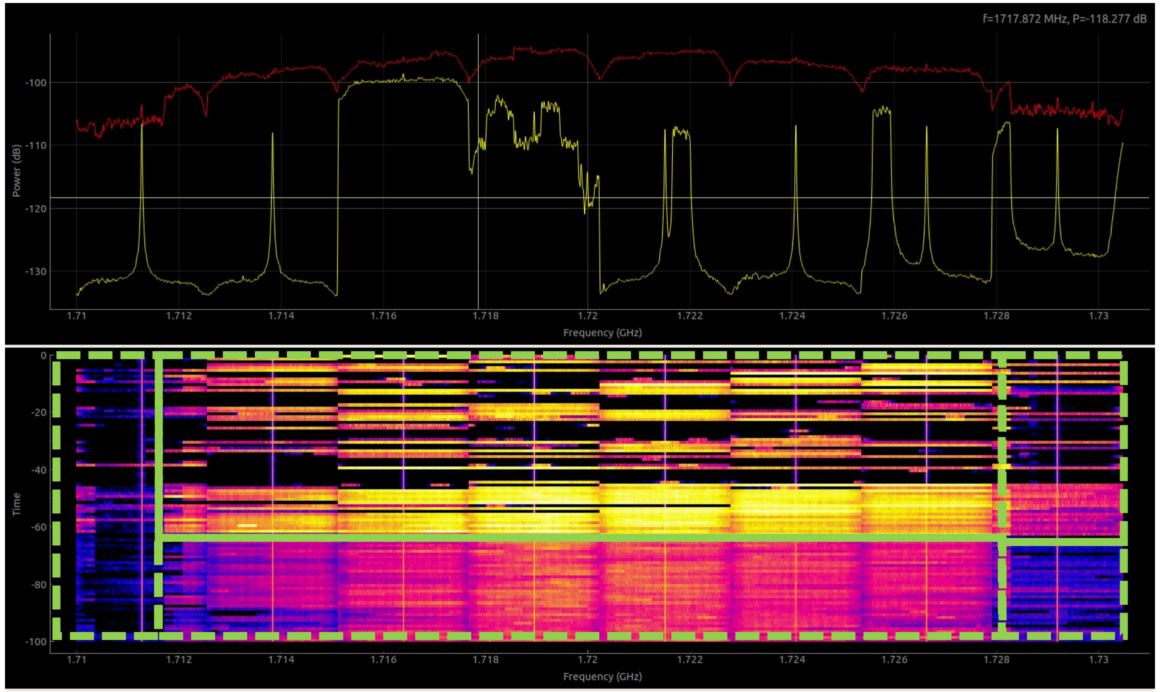


SVM Illustration by D. Unzueta, online

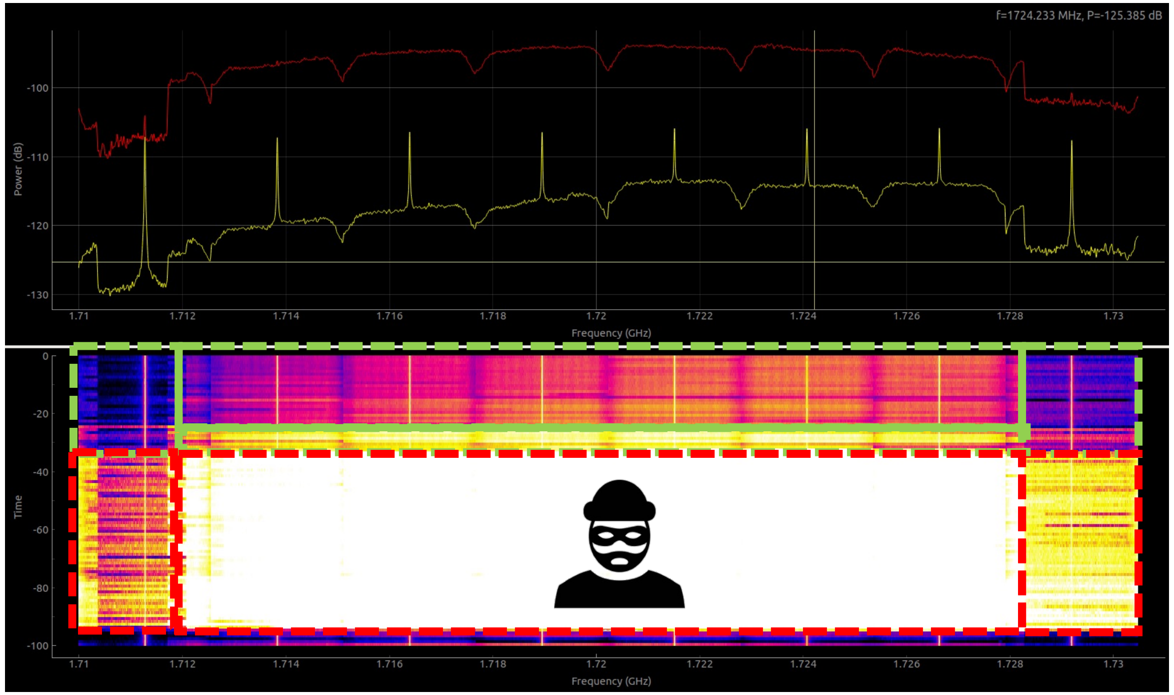
SID: A simple example

SDR-based RF Scanner

- Lab measurements of Scanner 1’s 5G uplink signal at a 1720 MHz carrier with 20 MHz bandwidth
- Upper plot: Power Spectral Density (received mW/Hz)
- Lower plot: Spectrogram of the same signal (x in Hz, y in s, color is received power)

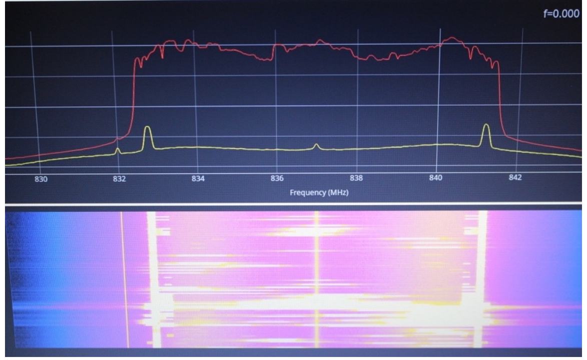


5G uplink signal with sparse traffic



5G uplink signal with rogue signal from 30 to 97 s

A watchdog for 5G: Discussion



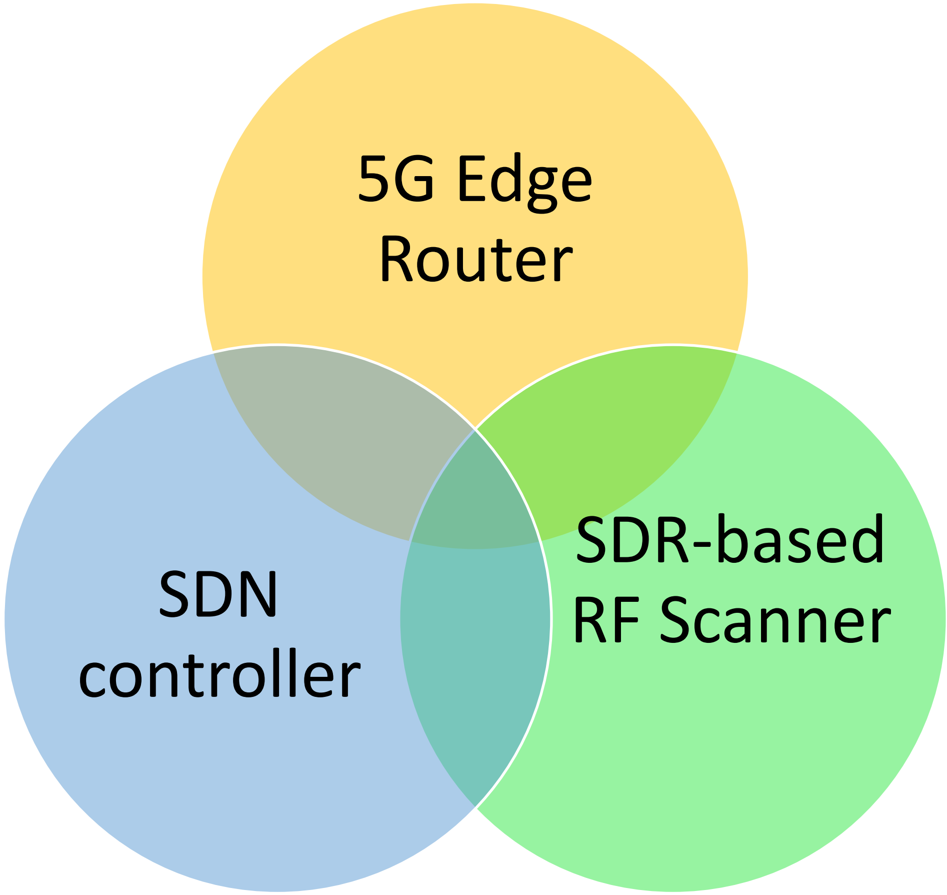
Pros

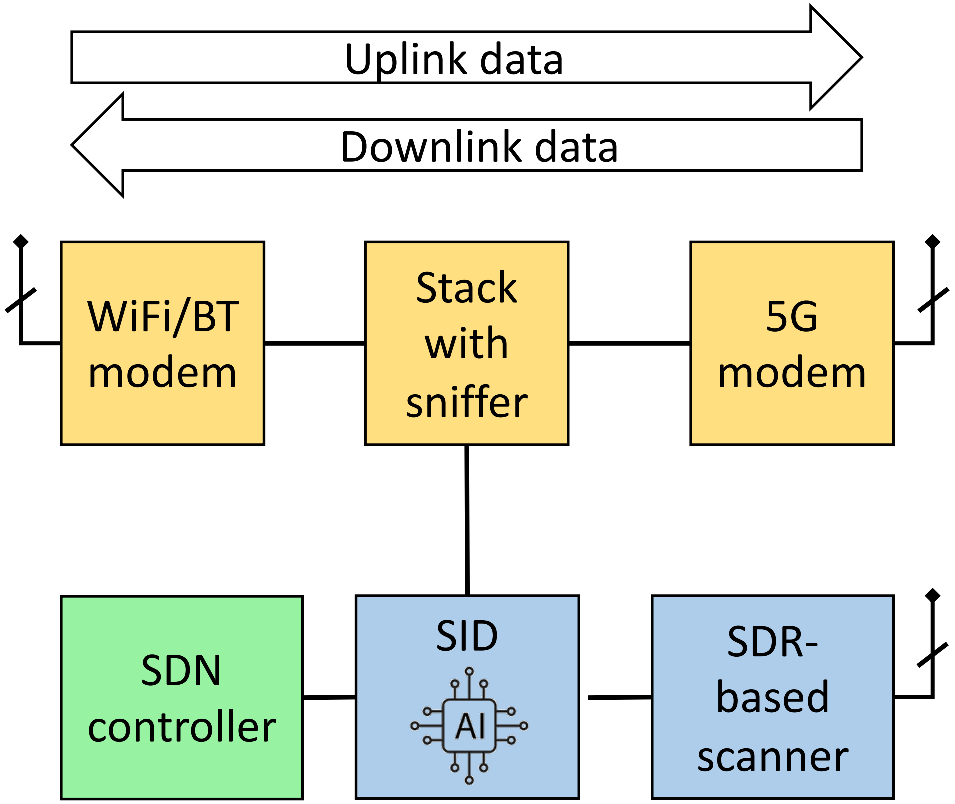
- Fundamental approach grounded in physics
  - Simplifies detection: Radio signals are bound by the laws of physics
  - Simplifies generalization: Many different attacks produce similar “rogue” signals
  - Complicates evasion: many attacks have to use physical signals
- Not done so far:
  - Wireless Intrusion Prevention System (WIPS) are not new [4] but stay at bit level
  - ML for intrusion detection is not new but stays at bit level [5, 6]
  - We bring ideas from radar and RF anomaly detection [7, 8] into IT security domain

Cons

- No logical analysis of the attack
  - Planned: Coupling with packet sniffer to better differentiate regular from irregular transmissions
  - Relating logical to physical signal may be sometimes complicated
- Quis custodiet ipsos custodes?
  - (or: Why to trust the watchdog?)
  - **Software-Defined Radio (SDR)!** Scanner entirely implemented in software
  - Minimal attack surface: Quite certain that SDR-hardware can only communicate with our code

Scanner 1: System design

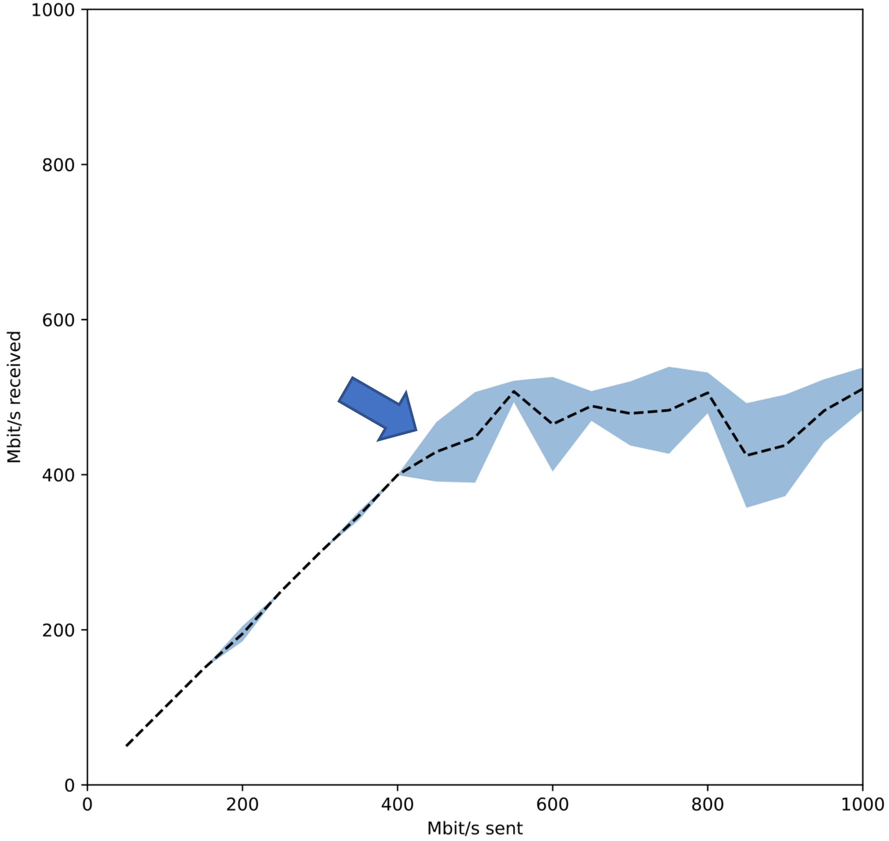




Scanner 1: Initial measurements

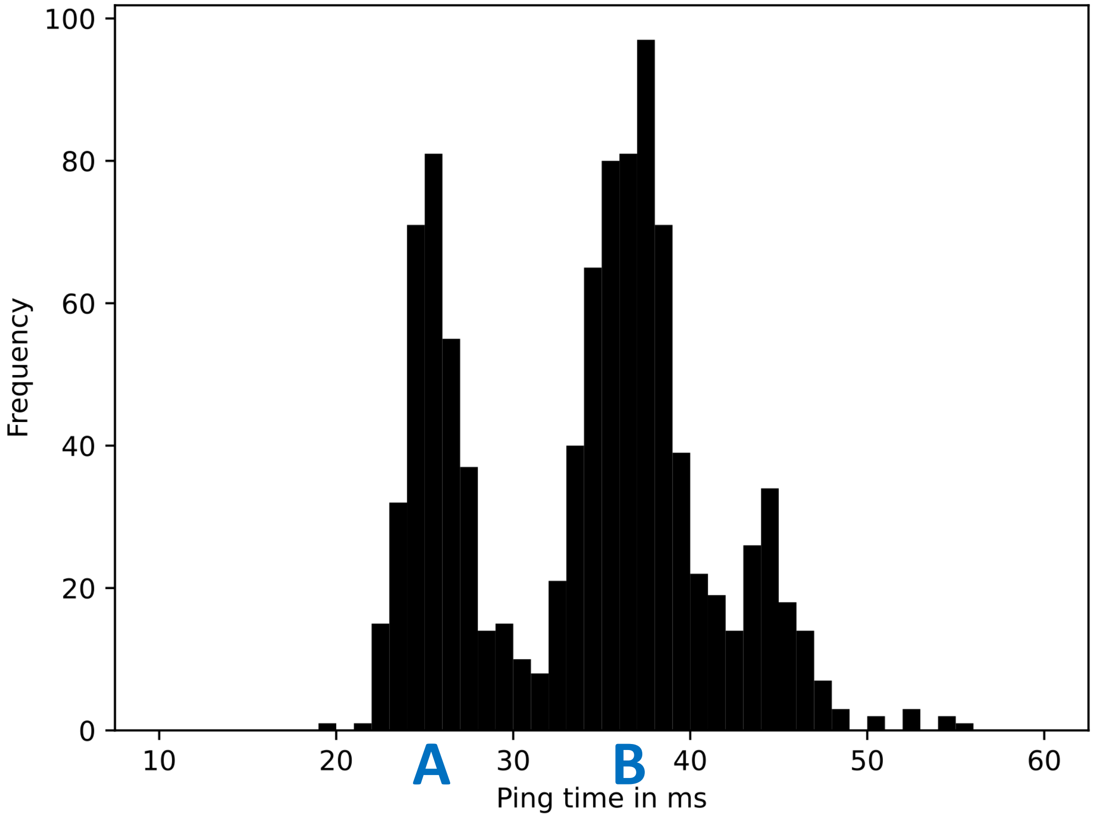
5G Edge Router

I/O plot with 95% confidence intervals



5G Downlink, TCP throughput im Mbit/s

Histogram of 1000 samples



5G, ICMP round-trip-time in ms

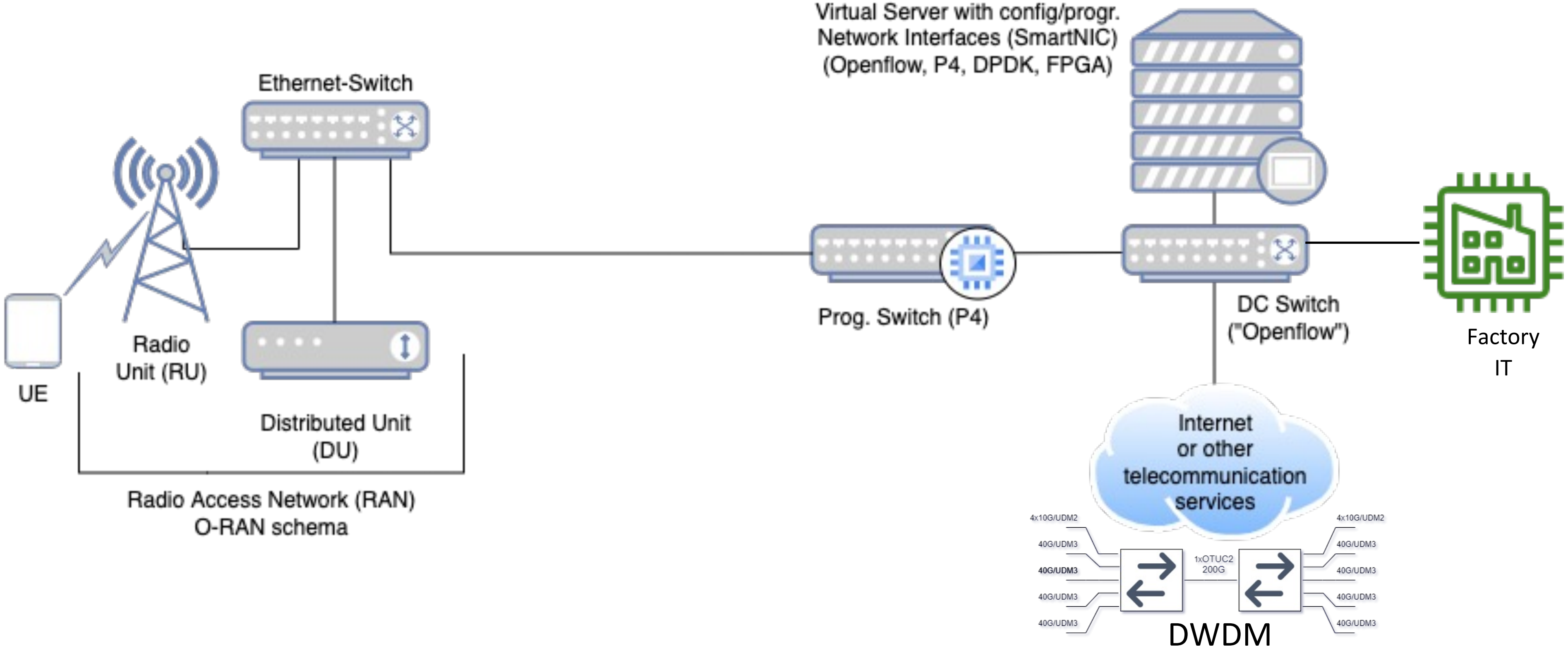
Scanner 1: Automation

SDN controller

- 5G networks lack full automation
  - Setup of or changes in the network, monitoring
  - Manual intervention needed
    - requires skilled workers
    - Expensive in budget and time
  - If available, only for single vendor!

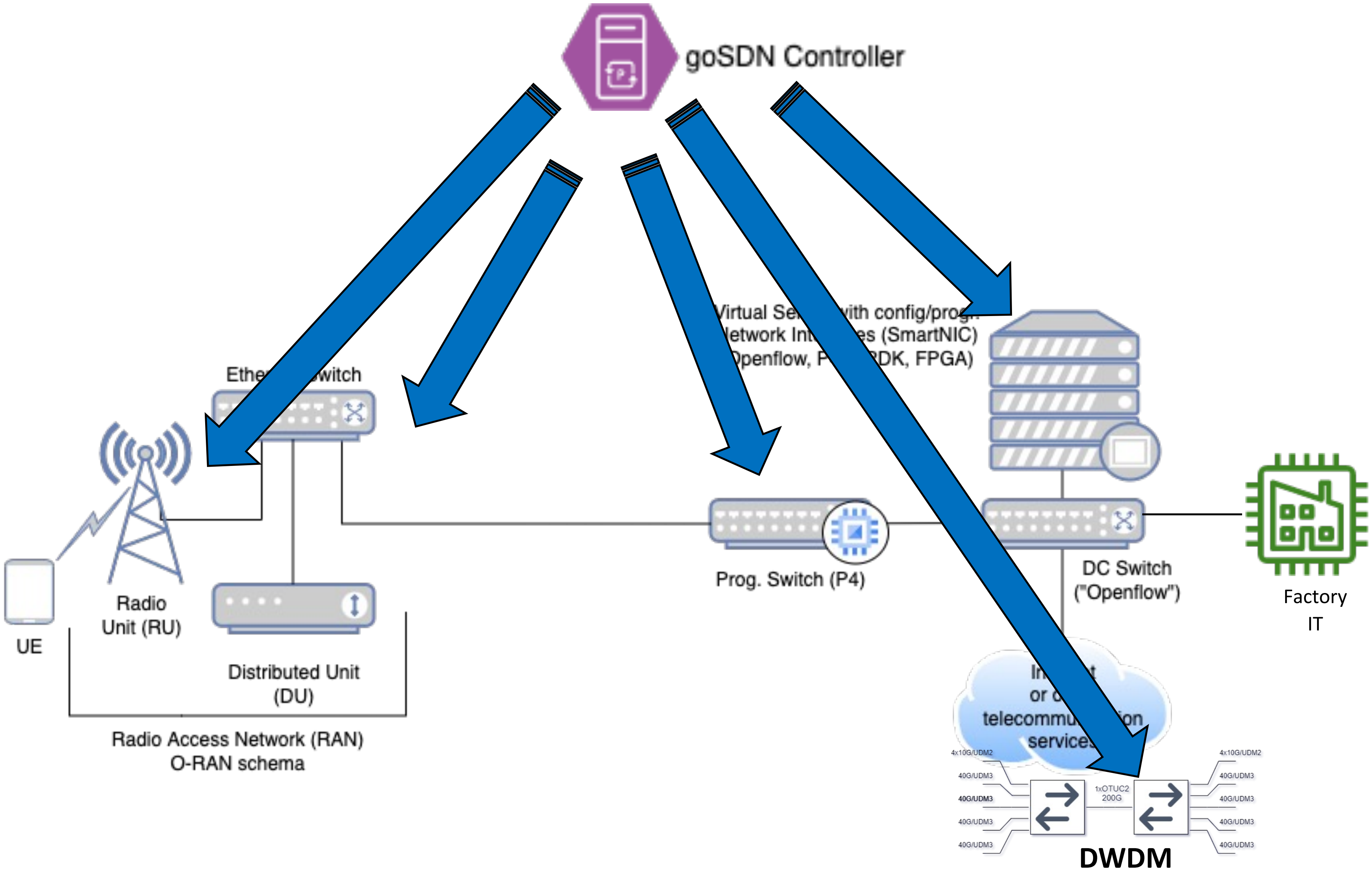
- Our SDN controller for automation and Zero-Trust
  - based on open-source goSDN controller
  - Automation of network management (FCAPS)
  - Zero-Trust management of all components
    - from 5G modem
    - to backhaul and core

A simple 5G Campus Network



OTN Figure: By EidenNor - Own work, CC BY-SA 4.0,
https://commons.wikimedia.org/w/index.php?curid=112147710

Controller: Automated zero-trust management



Trailblazer Networks

- Spin-off of the da/net research group
  - Reliable and trustworthy 5G/6G and fixed networks
  - Founders: Malte Bauch, Michael Birger, Martin Stiemerling, and Stefan Valentin

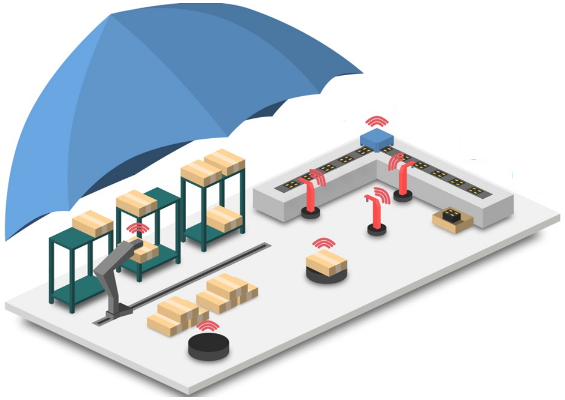
- Initial project 5G-Multi-Service-Router (5G-MSR)
  - Funded by *Federal Agency for Disruptive Innovation SPRIND*
  - Nov 21 to Nov 22

- Now: Extending the 5G-MSR towards Scanner-1

Summary and next steps

- Cellular network security and automation is still in the

- Scanner 1 – Our wireless shield for private 5G networks:
  - is a powerful edge router for private 5G networks
  - protects these networks at a physical level
  - includes an SDN controller for incident response and further automation



- We have a solid concept, plugged it together and see that it works
  - Field tests in industrial 5G network coming in October with CONGIV YOUR E2E NETWORK SPECIALIST MUGLER TELCO NETWORKS.
  - More ideas: Logical analysis, radio bearing of attacker signal, retaliation
- **Now we need further collaborators and more funding! ☺**

References

[1] Bundesnetzagentur “Übersicht der Zuteilungsinhaber für Frequenzzuteilungen für lokale Frequenznutzungen im Frequenzbereich 3.700-3.800 MHz”, Online, May 2022.

[2] Reuters, “Abhörskandal gegen Merkel weitet sich aus”, online, Oct. 2013.

[3] Statista, “Number of 5G subscriptions worldwide from 2019 to 2027”, online, Feb. 2022.

[4] Yujia Zhang et al. “An overview of wireless intrusion prevention systems”. *In Proc. of IEEE Int. Conf. on Communication Systems, Networks and Applications, vol*. 1., 2010.

[5] M. A. Elsadig und A. Gafar, “Covert Channel Detection: Machine Learning Approaches”, *IEEE Access*, no. 10, 2022.

[6] Taeshik Sohn, JungTaek Seo, and Jongsub Moon. “A study on the covert channel detection of TCP/IP header using support vector machine”, in Proc. of Int. Conf. on Information and Communications Security, 2003.

[7] K. Youssef et al. “Machine Learning Approach to RF Transmitter Identification”, *IEEE Journal of Radio Frequency Identification,* vol. 2, no. 4, 2018.

[8] J. Lu et al. “Machine-Learning PUF-based Detection of RF Anomalies in a Cluttered RF Environment”, in *Proc. of IEEE Int. Symp. on Technologies for Homeland Security (HST)*, 2021.

Trailblazer
networks

sv@tbnet.works
mls@tbnet.works