Exploiting 5G for Covert Channels: But what about Open RAN?

Markus Walter Federal Office for Information Security (BSI)

Federal Office
for Information Security

BSI as the **Federal Cyber Security Authority**
shapes information security in digitization through prevention, detection and reaction
for government, business and society.

Competence Center 5G/6G

- Security guidelines for national 5G network operators
- ***5G/6G Security Lab***: Analysis and evaluation of vulnerabilities and attack vectors
- ***Standardization*** and ***certification***: Cooperation in international committees (e.g. ENISA, 3GPP, ETSI)
- Cooperation with R&D, vendors and MNOs

Federal Office
for Information Security

What exactly is a Covert Channel?

- Covert channels hide existence of data transmission between covert sender and receiver
- Originally not intended for transferring data
- Network covert channels categorized by taxonomy of Wendzel et al.:

Covert Timing Pattern									
Protocol-agnostic			Protocol-aware						
Inter-packet Times	Message Timing	Rate/ Throughput	Artificial Loss	Message (PDU) Ordering	(Artificial) Retransmission	Frame Collisions	Temperature	Artificial Reconnections	Artificial Resets

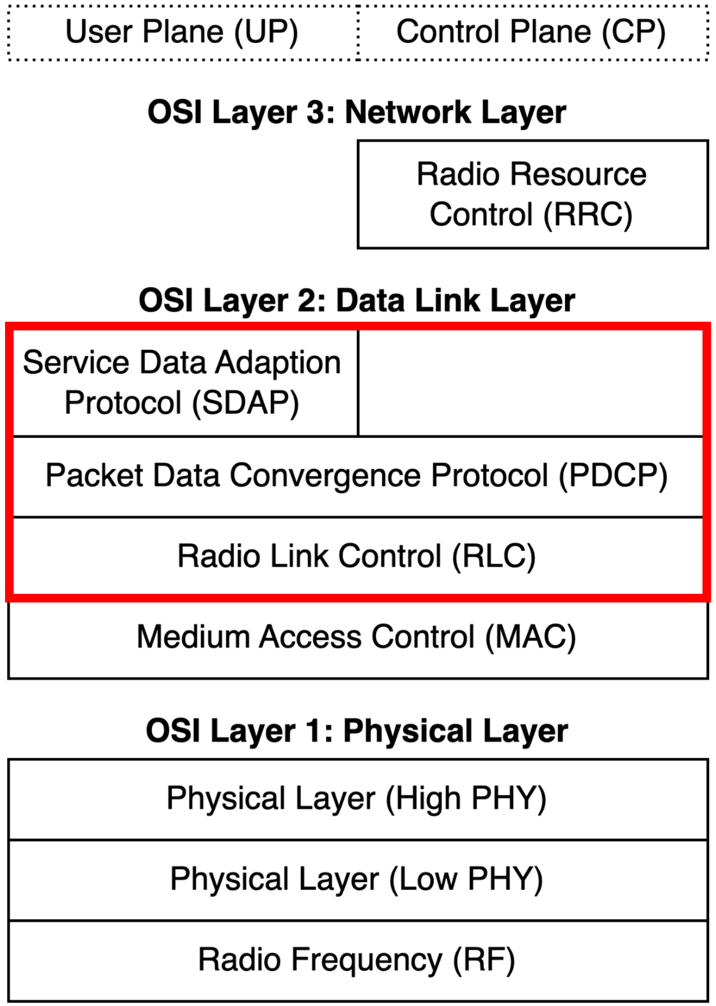
Covert Storage Pattern									
Modification of Non-Payload (Data in protocol-specific fields)						Modification of Payload (User Data)			
Structure Modifying			Structure Preserving			User-data Agnostic		User-data Aware	
Size Modulation	Sequence	Add Redundancy	Random Value	Value Modulation	Reserved/ Unused	Payload Field Size Modulation	User-data Corruption	Modify Redundancy	User-data Value Modulation & Reserved/Unused

Federal Office for Information Security

Steffen Wendzel et al. “Pattern-Based Survey and Categorization of Network Covert Channel Techniques”. 2015. https://doi.org/10.1145/2684195
Steffen Wendzel. 2015-Taxonomy (Networking). 2022. https://patterns.ztt.hs-worms.de/NIHPattern/

5G New Radio

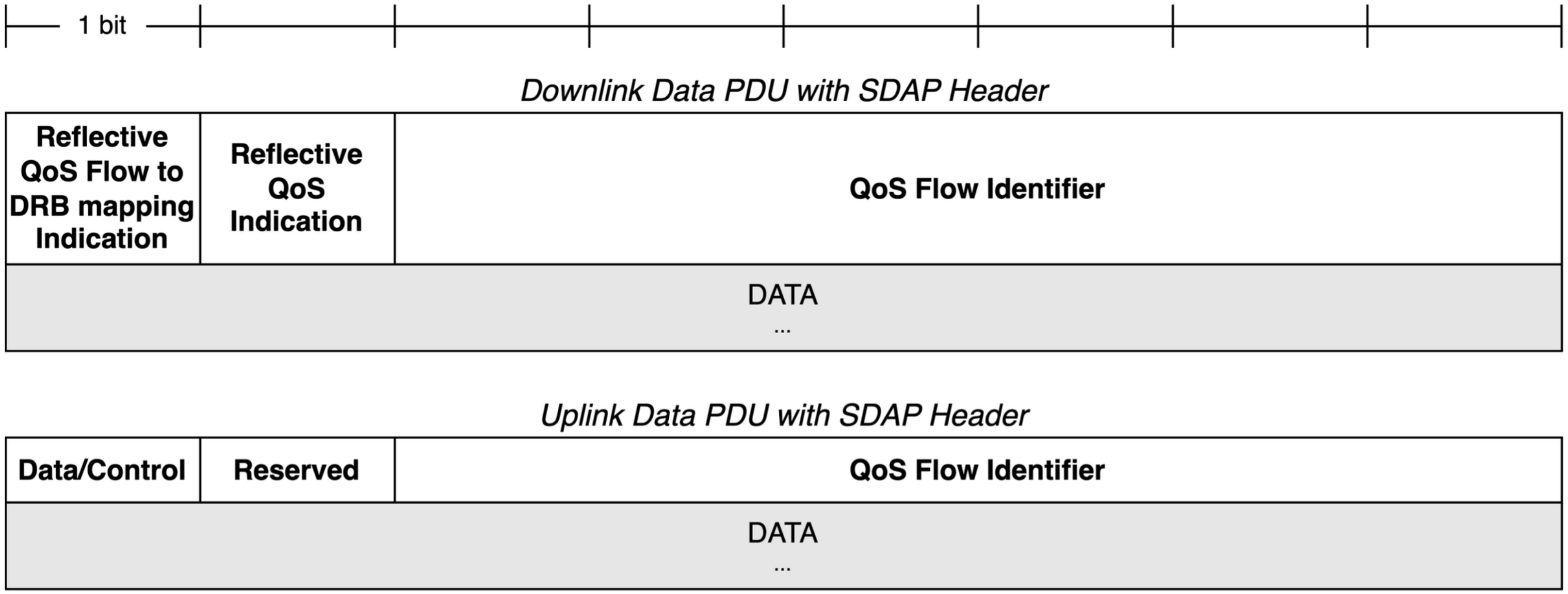
- **RRC**: Procedures for establishment, configuration and management of radio link between base station and UE
- **SDAP**: Quality of Service (QoS) management
- **PDCP**: Merge of CP and UP payload as well as encryption and integrity protection
- **RLC**: Procedures for segmentation and retransmissions
- **MAC**: Procedures for random access and error correction
- **PHY**: Procedures for physical data transmission on uplink/downlink



Federal Office for Information Security

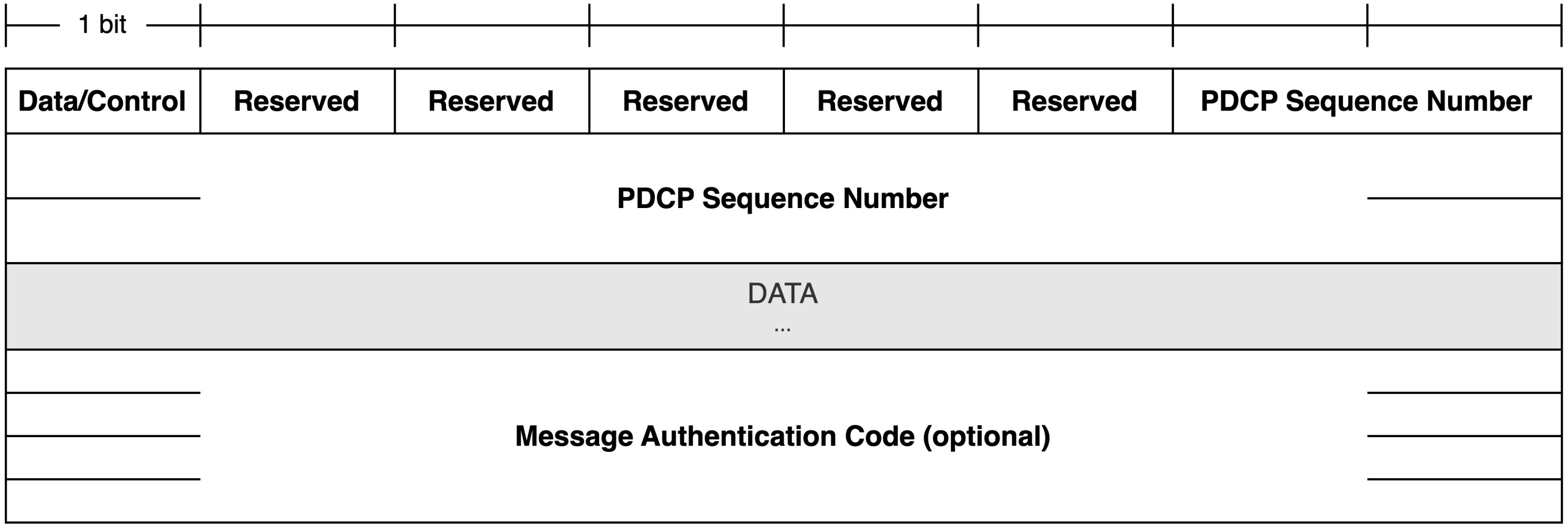
Protocol Analysis – Service Data Adaption Protocol (SDAP)

- Header consists mostly of QoS Flow Identifier
- Only 1 reserved bit in header of uplink PDU
- SDAP is less suitable for hiding information → **SDAP is not considered further**



Protocol Analysis – Packet Data Convergence Protocol (PDCP)

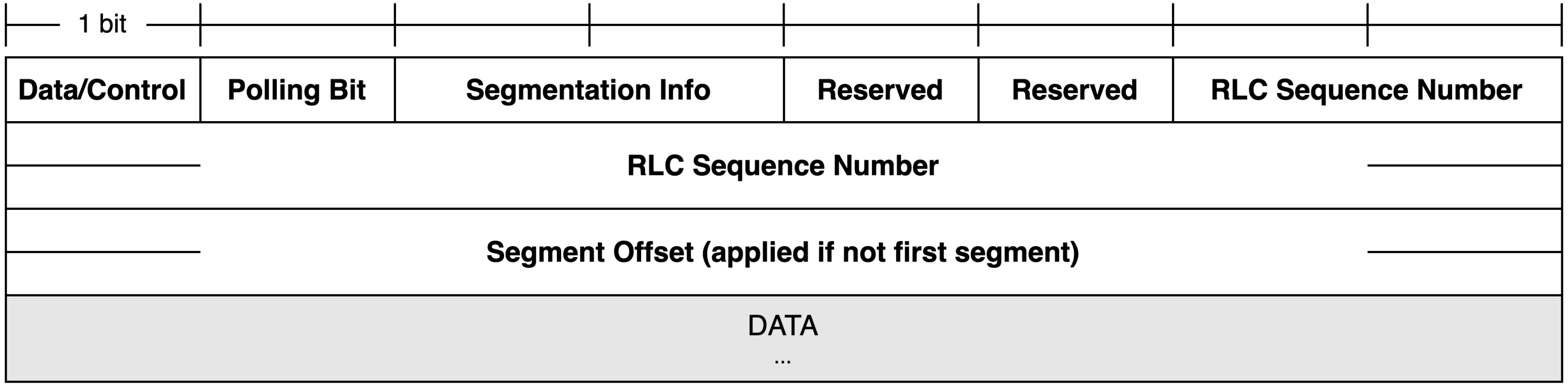
- Exploitation of Sequence Number is feasible → high risk of detection
- Exploitation of MAC field is possbile, but only if integrity protection is configured by RRC
- PDCP has 5 reserved bits → **good basis for hiding information**



PDCP Data PDU for Data Radio Bearer (18 Bit Sequence Number)

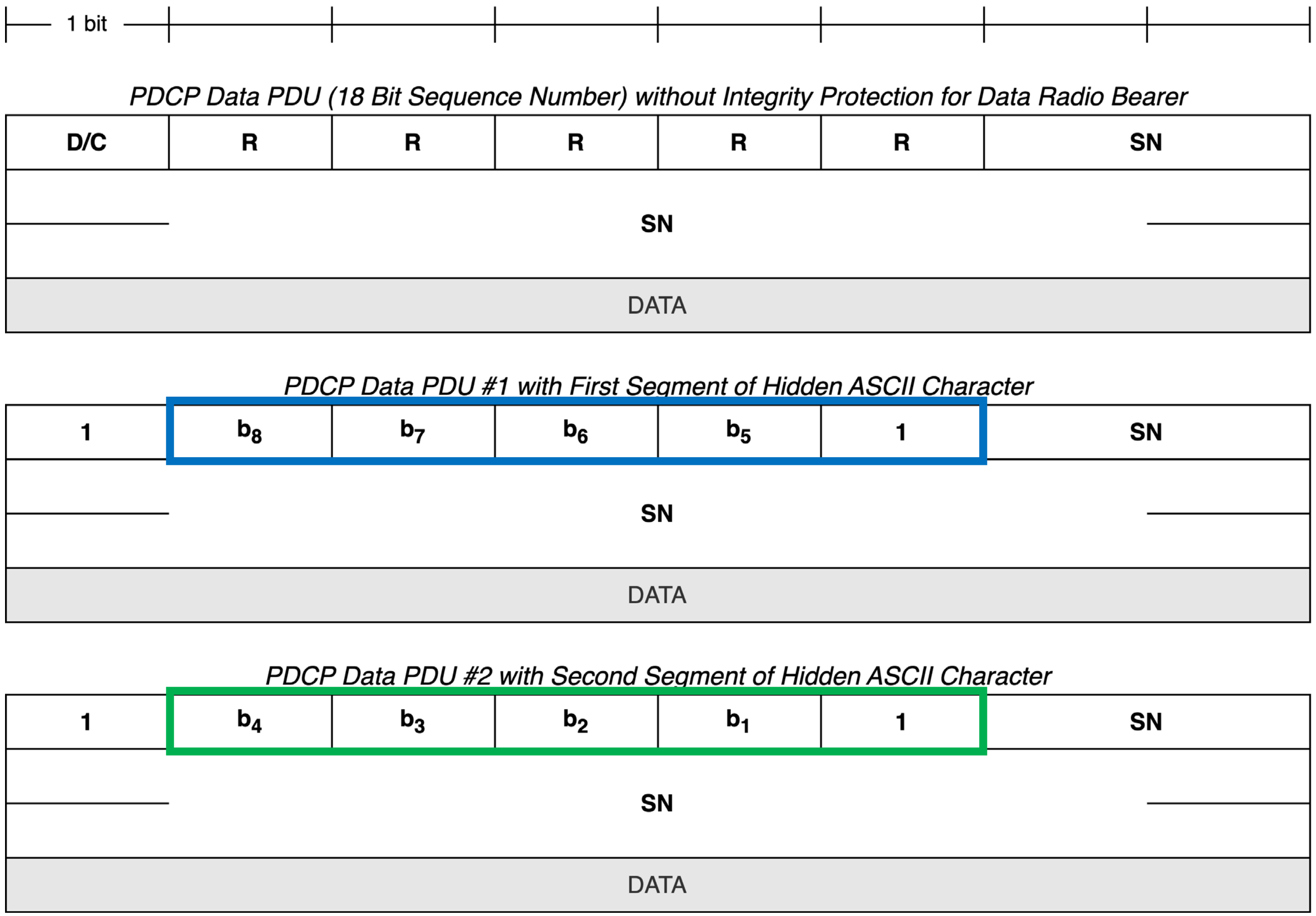
Protocol Analysis – Radio Link Control (RLC)

- RLC has plenty of header elements to exploit
- Sequence Number and Segment Offset can be utilized to encode covert data
  → most likely affects functionality → high risk of detection
- Header contains 2 reserved bits → **Could probably be used in addition to PDCP**

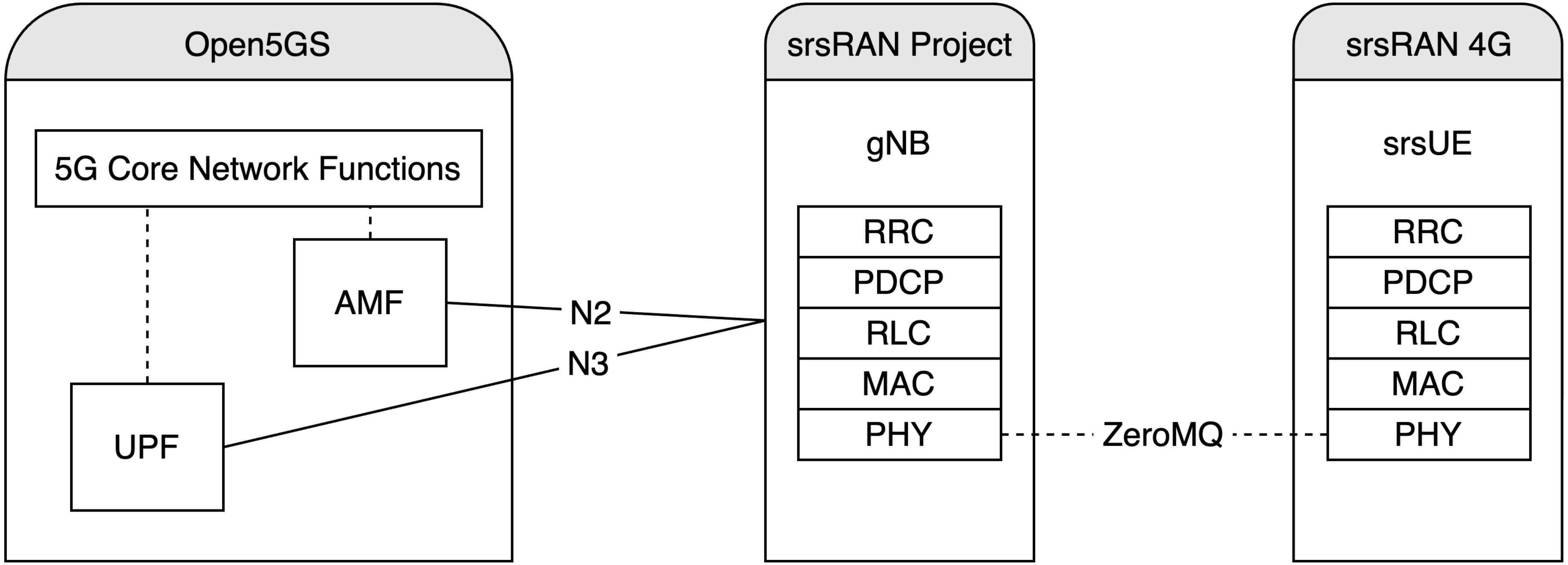


RLC AM PDU with Segmentation (18 Bit Sequence Number)

Transmission of ASCII Characters over a Covert Channel



Proof of Concept with Virtualized Test Environment



Federal Office
for Information Security

Covert Sender

```
    if (covert_timer == 10) {
        covert_timer = 1;
        if (input.length() > 0) {
            if (transmitted_segment_ctr % 2 == 0) {
                // 0xf0 = 11110000
                char_segment = 0xf0 & input[0];
                // 0x84 = 10000100
                first_header_byte = 0x84 | (char_segment >> 1);
            } else {
                // 0x0f = 00001111
                char_segment = 0x0f & input[0];
                // 0x84 = 10000100
                first_header_byte = 0x84 | (char_segment << 3);
                input.erase(0,1);
            }
            transmitted_segment_ctr++;
        }
    } else {
        covert_timer++;
    }

    // Hiding method is applied if PDU is Data PDU
    if (is_drb()) {
        hdr_writer.append(first_header_byte);
    } else {
        hdr_writer.append(0x00);
    }
```

Covert Receiver

```
// File: srsRAN_Project/lib/pdcp/pdcp_entity_rx.cpp
bool pdcp_entity_rx::read_data_pdu_header(pdcp_data_pdu_header& hdr, const byte_buffer_chain& buf) const
{
    ...
    byte_buffer_chain::const_iterator buf_it = buf.begin();

    // 0x04 = 00000100
    if ((*buf_it & 0x04U) == 4) {
        if (received_segment_ctr % 2 == 0) {
            // 0x78 = 01111000
            uint8_t covert_data_bits = (*buf_it & 0x78U) << 1;
            assembled_byte = covert_data_bits;
        } else {
            // 0x78 = 01111000
            uint8_t covert_data_bits = (*buf_it & 0x78U) >> 3;
            assembled_byte |= covert_data_bits;
            char assembled_char = (char) assembled_byte;
            assembled_byte = 0;
            output += assembled_char;
            write_to_file(output_file ,assembled_char);
        }
        received_segment_ctr++;
    }
    ...
}
```

gNodeB (Covert Sender)

mawa@temis: ~/srsRAN_Project/configs

```
--== srsRAN gNB (commit 1afd7240f) ==--

Connecting to AMF on 127.0.0.5:38412
Available radio types: uhd and zmq.
Cell pci=1, bw=10 MHz, dl_arfcn=368500 (n3), dl_freq=1842.5 MHz, dl_ssb_arfcn=368410, ul_freq=1747.5 MH
z

==== gNodeB started ===
Type <t> to view trace
t

           ----------------DL---------------|------------------UL-------------------
 pci rnti  cqi  ri  mcs  brate   ok  nok  (%) | pusch  mcs  brate   ok  nok  (%)    bsr
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1    0      0    0    0   0% |   n/a    0      0    0    0   0%    0.0
   1 4601   15   1   28   669k   42    0   0% |  65.5   26    76k   29    0   0%    0.0
   1 4601   15   1   28   1.1M   52    0   0% |  65.5   28    79k   17    0   0%    0.0
   1 4601   15   1   28   1.1M   56    0   0% |  65.5   27    73k   21    0   0%    0.0
   1 4601   15   1   28   1.1M   52    0   0% |  65.5   27    79k   17    0   0%    0.0
```

UE (Covert Receiver)

mawa@temis: ~/srsRAN_4G/srsue

```
mawa@temis:~/srsRAN_4G/srsue$ sudo srsue ue_zmq.conf
Active RF plugins: libsrsran_rf_uhd.so libsrsran_rf_zmq.so
Inactive RF plugins:
Reading configuration file ue_zmq.conf...

Built in Release mode using commit fa56836b1 on branch master.

Opening 1 channels in RF device=zmq with args=tx_port=tcp://127.0.0.1:2001,rx_port=tcp://127.0.0.1:
2000,base_srate=11.52e6
Supported RF device list: UHD zmq file
CHx base_srate=11.52e6
Current sample rate is 1.92 MHz with a base rate of 11.52 MHz (x6 decimation)
CH0 rx_port=tcp://127.0.0.1:2000
CH0 tx_port=tcp://127.0.0.1:2001
Current sample rate is 11.52 MHz with a base rate of 11.52 MHz (x1 decimation)
Current sample rate is 11.52 MHz with a base rate of 11.52 MHz (x1 decimation)
Waiting PHY to initialize ... done!
Attaching UE...
Random Access Transmission: prach_occasion=0, preamble_index=0, ra-rnti=0x39, tti=334
Random Access Complete.     c-rnti=0x4601, ta=0
RRC Connected
PDU Session Establishment successful. IP: 10.45.0.26
RRC NR reconfiguration successful.
```

Overt Traffic

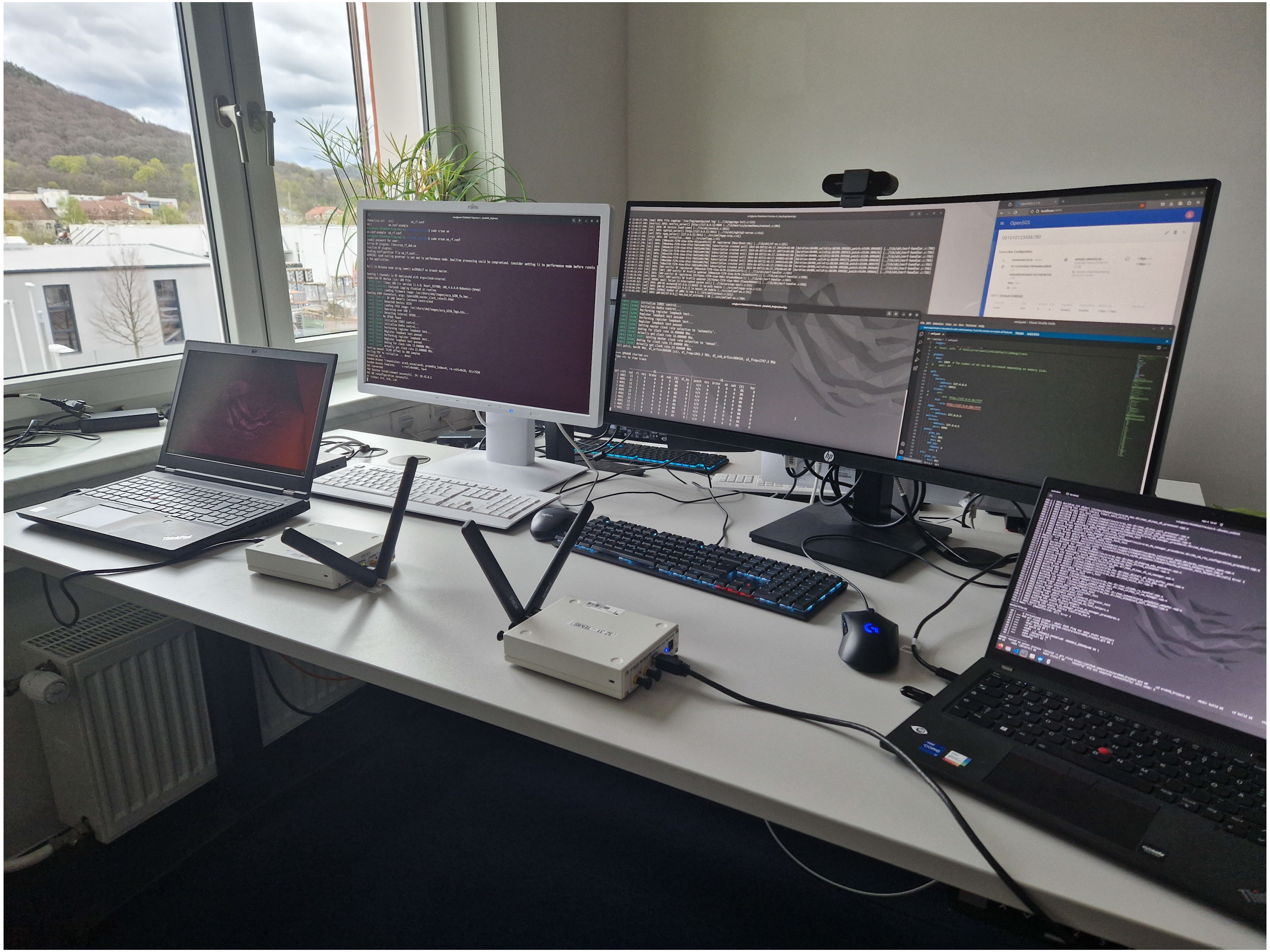
mawa@temis: ~

```
mawa@temis:~$ iperf3 -c 10.45.0.26 -b 1M
Connecting to host 10.45.0.26, port 5201
[  5] local 10.45.0.1 port 43250 connected to 10.45.0.26 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   204 KBytes  1.67 Mbits/sec    0   38.2 KBytes
[  5]   1.00-2.00   sec   128 KBytes  1.05 Mbits/sec    0   38.2 KBytes
[  5]   2.00-3.00   sec   128 KBytes  1.05 Mbits/sec    0   39.5 KBytes
[  5]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec    0   40.8 KBytes
[  5]   4.00-5.00   sec   128 KBytes  1.05 Mbits/sec    0   42.1 KBytes
[  5]   5.00-6.00   sec   128 KBytes  1.05 Mbits/sec    0   44.8 KBytes
[  5]   6.00-7.00   sec   128 KBytes  1.05 Mbits/sec    0   39.5 KBytes
[  5]   7.00-8.00   sec   128 KBytes  1.05 Mbits/sec    0   26.3 KBytes
[  5]   8.00-9.00   sec  0.00 Bytes  0.00 bits/sec    0   47.4 KBytes
[  5]   9.00-10.00  sec   128 KBytes  1.05 Mbits/sec    1   50.0 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  1.20 MBytes  1.01 Mbits/sec    1             sender
[  5]   0.00-10.04  sec  1.20 MBytes  1.00 Mbits/sec                  receiver
```

UE Log

mawa@temis: ~

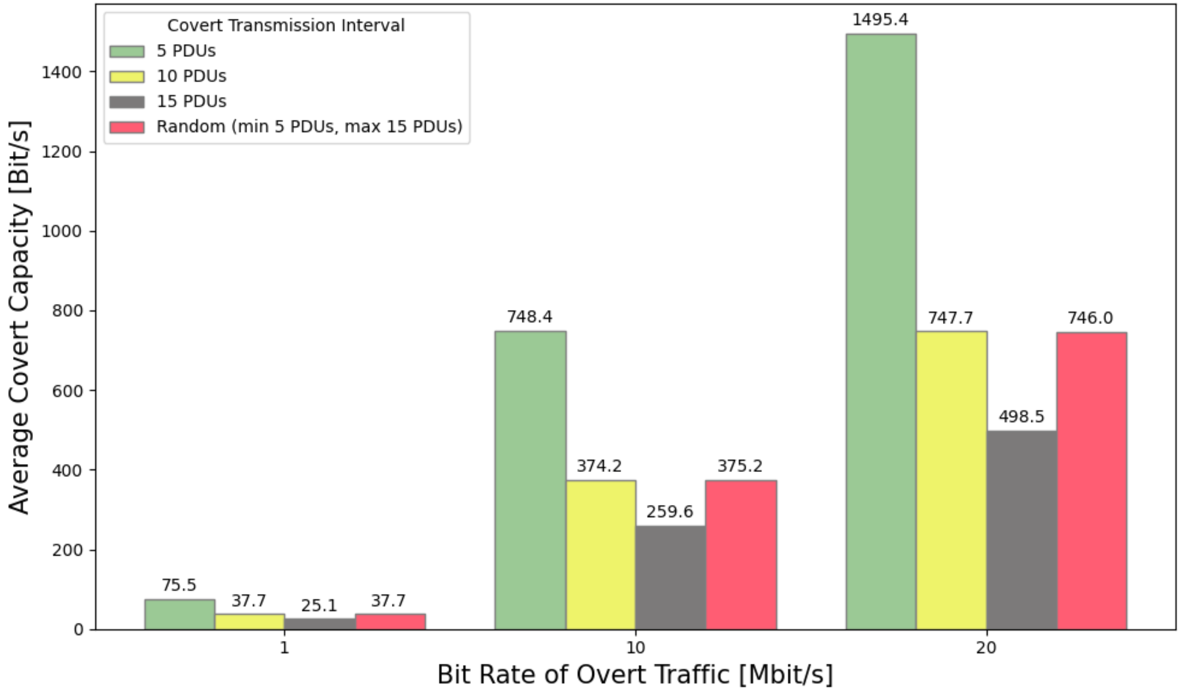
```
mawa@temis:~$ tail -f /tmp/ue.log | grep Extracted
2023-09-27T16:32:32.377724 [PDCP-NR] [I] Extracted message: S
2023-09-27T16:32:32.424129 [PDCP-NR] [I] Extracted message: Se
2023-09-27T16:32:32.442636 [PDCP-NR] [I] Extracted message: Sec
2023-09-27T16:32:33.004907 [PDCP-NR] [I] Extracted message: Secr
2023-09-27T16:32:33.039361 [PDCP-NR] [I] Extracted message: Secre
2023-09-27T16:32:33.055898 [PDCP-NR] [I] Extracted message: Secret
2023-09-27T16:32:33.064235 [PDCP-NR] [I] Extracted message: Secret
2023-09-27T16:32:33.080149 [PDCP-NR] [I] Extracted message: Secret m
2023-09-27T16:32:34.053930 [PDCP-NR] [I] Extracted message: Secret me
2023-09-27T16:32:34.115123 [PDCP-NR] [I] Extracted message: Secret mes
2023-09-27T16:32:34.133653 [PDCP-NR] [I] Extracted message: Secret mess
2023-09-27T16:32:34.150480 [PDCP-NR] [I] Extracted message: Secret messa
2023-09-27T16:32:34.162074 [PDCP-NR] [I] Extracted message: Secret messag
2023-09-27T16:32:35.103511 [PDCP-NR] [I] Extracted message: Secret message
2023-09-27T16:32:35.149011 [PDCP-NR] [I] Extracted message: Secret message!
2023-09-27T16:32:35.164563 [PDCP-NR] [I] Extracted message: Secret message!
```



Federal Office
for Information Security

Evaluation of the Covert Channel within PDCP

- Reliability is ensured by PDCP
  → Robust against normal channel noise
- Covert capacity depends on:
  – Bandwidth of overt traffic (proportional)
  – Interval of covert transmission (proportional)
- Randomized intervals improve undetectability
- Practical example:
  Broadband transmission (20 Mbps, 60 seconds)
  → 815 words (5600 characters)



Federal Office
for Information Security

Detection of the Covert Channel

1) Detection within **base station** or **User Equipment**
   - Unrestricted access to protocol layer
   - Logging or network analyzer
2) Detection on **air interface**
   - Only possible if encryption is not activated
   - Knowledge of radio parameters necessary
   - Not possible over a large area

```
> Frame 107: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
  DLT: 149, Payload: udp (User Datagram Protocol)
> User Datagram Protocol, Src Port: 48879, Dst Port: 57005
v MAC-NR DL-SCH (LCID:4 90 bytes) (Padding 52 bytes)
  > [Context (RNTI=17921)]
  > Subheader: (LCID:4 90 bytes)
  v RLC-NR [DL] [AM] DRB:1  [DATA] (P) SN=12                [87-bytes]
    > [Context]
    > AM Header  (P) SN=12
      AM Data: c4000c4500005403fc00004001624c0a2d00010a2d00070000bc053a4b000df084046500…
    v PDCP-NR (SN=12    )
      v [Configuration:    DRB-1  (direction=Downlink, plane=User)]
          [Direction: Downlink (1)]
          [Plane: User (2)]
          [Bearer type: DCCH (1)]
          [Bearer Id: 1]
          [Seqnum length: 18]
          [MAC-I Present: False]
          [SDAP header: Not Present]
          [ROHC Compression: False]
      > [UE Security (ciphering=NEA0 (NULL), integrity=NIA2 (AES))]
        1... .... = PDU Type: Data PDU
      v .100 01.. = Reserved: 0x11
        v [Expert Info (Error/Malformed): Reserved bits have value 0x11 - should be 0x0]
            [Reserved bits have value 0x11 - should be 0x0]
            [Severity level: Error]
            [Group: Malformed]
        .... ..00 0000 0000 0000 1100 = Seq Num: 12
      > [Sequence Analysis - OK]
      > Internet Protocol Version 4, Src: 10.45.0.1, Dst: 10.45.0.7
      > Internet Control Message Protocol
  > Subheader: (Padding 52 bytes)
```

Federal Office for Information Security

How to Prevent the Covert Channel?

3GPP TS 38.323 version 17.5.0 Release 17 39 ETSI TS 138 323 V17.5.0 (2023-07)

6.3.6 R

Length: 1 bit

Reserved. In this version of the specification reserved bits shall be set to 0. Reserved bits shall be ignored by the receiver.

```
// File: srsRAN_4G/lib/src/pdcp/pdcp_entity_base.cc
uint32_t pdcp_entity_base::read_data_header(const unique_byte_buffer_t&
↪ pdu) {
    ...
    if ((pdu->msg[0] & 0x7CU) != 0) { // 0x7C = 01111100
        logger.warning("Malformed PDCP Header. Reserved bits are set");
        pdu->msg[0] &= 0x83; // 0x83 = 10000011
    }
    ...
}
```

Federal Office
for Information Security

But what about Open RAN?

- New interfaces and components in O-RAN with Application Protocols, Service Models and Message Flows (OFH, A1, E2, O1, O2, Y1, …)

→ Many possibilities to create covert channels!

- Example: Reserved bits in OFH

5.1.3.1.2 ecpriReserved (eCPRI reserved)

Description: This parameter is reserved for eCPRI future use. NOTE: This parameter is part of the eCPRI common header.

Value range: {001b-111b=Reserved}.

Type: unsigned integer

Field length: 3 bits.

Default Value: 000b (reserved fields should always be set to all zeros).

Table 5-1 : eCPRI Transport Header Field Definitions

Section Type : any									
0 (msb)	1	2	3	4	5	6	7 (lsb)	# of bytes	
ecpriVersion				ecpriReserved			ecpriConcatenation	1	Octet 1
ecpriMessage								1	Octet 2
ecpriPayload								2	Octet 3
ecpriRtcid / ecpriPcid								2	Octet 5
ecpriSeqid								2	Octet 7

Good News: There is a test! Bad News: …?

Test Name: TC_FH_U-PLANE_MALFORMED_PACKET

Test description and applicability

Purpose: The purpose of this test is to verify the O-DU's ability to handle and reject malformed or invalid user plane packets.

Test setup and configuration

- A valid eCPRI connection between the O-RU and O-DU.

Test procedure

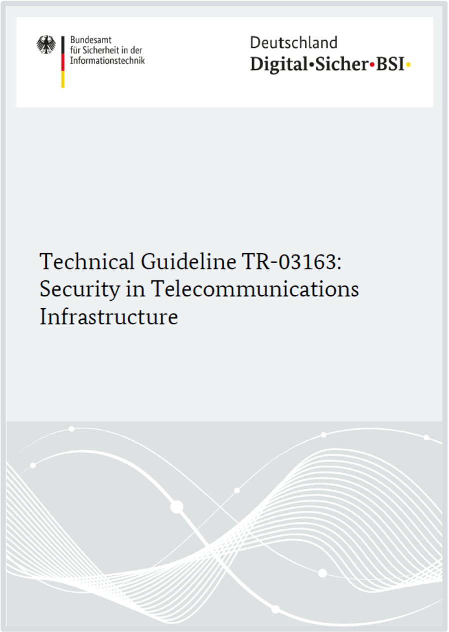
1. Generate a user plane packet with invalid or malformed data, such as incorrect headers, corrupted payload, or unsupported formats.
2. Transmit the malformed packet over the eCPRI.
3. Monitor the O-DU's response and behaviour.
4. Verify that the O-DU identifies and rejects the malformed packet.
5. Observe the impact on the O-DU, such as error messages, logging, or abnormal behavior.

Expected Results

- The O-DU detects and rejects malformed or invalid user plane packets.
- It handles the rejection gracefully without affecting normal operation.
- Appropriate error messages or log entries are generated.

Security through Certification

- Certification of critical network equipment in public 5G networks
  - Required by German law (§165 TKG) as of January 2026
  - By an authorized certification body → BSI
- Technical Guideline TR-03163: Security in Telecommunications Infrastructure → Selection of authorized certification schemes
- NESAS Cybersecurity Certification Scheme – German Implementation (CCS-GI)
  - Based on GSMA Network Equipment Security Assurance Scheme (NESAS)
- Security Assurance Specifications (SCAS)
  - Security Tests specified by 3GPP (TS 33.xxx)
  - Available for many 4G and 5G network functions

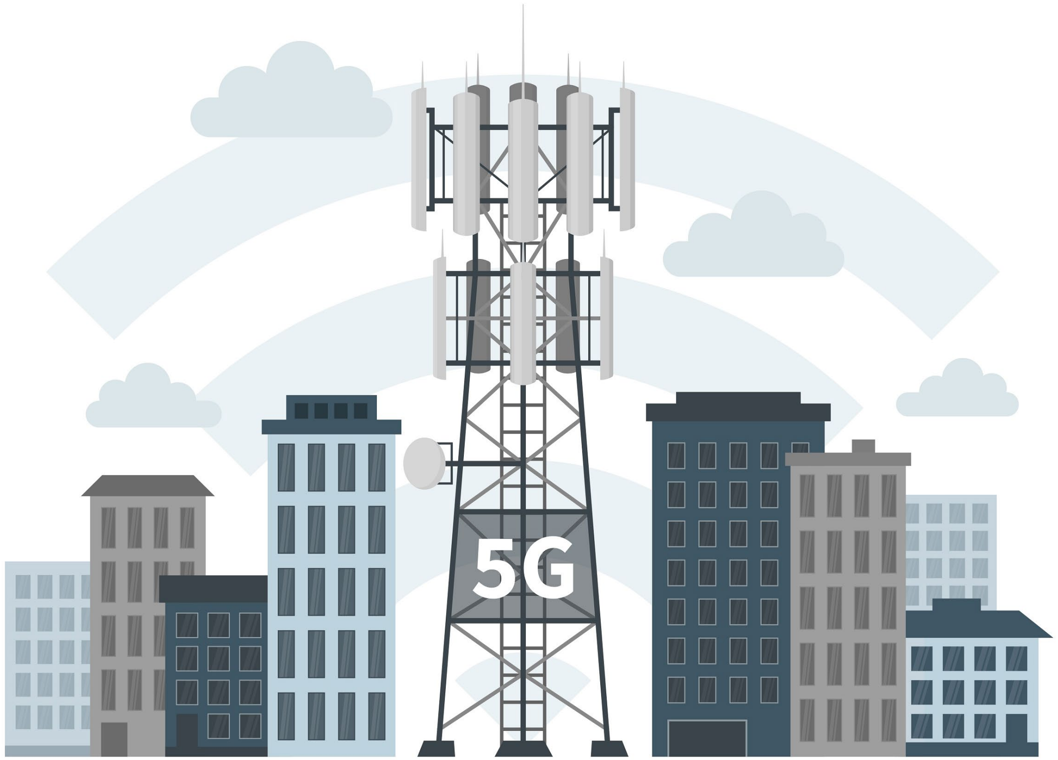


Summary

- Covert channels are feasible in 5G
- Exploitation of PDCP is the best option on the 5G air interface → Covert capacity can be high
- O-RAN can be exploited, too! → O-RAN Alliance needs to extend and clarify their security tests
- Enhancements and (practical) verification of Security Assurance Tests by BSI
  → Basis for certification of commercial 5G components
    1. Assurance of security measures
    2. Reduction of implementation flaws
- BSI continues standardization work in 3GPP, ETSI and GSMA NESAS Group
  → Current focus on enhancements of SCAS

Any Questions?

Deutschland
Digital•Sicher•BSI•



Contact

Markus Walter
Division S 31 – Security for 5G/6G Infrastructure

markus.walter@bsi.bund.de
referat-s31@bsi.bund.de

Federal Office for Information Security (BSI)
Hüttenstr. 14
01705 Freital
www.bsi.bund.de

Federal Office
for Information Security