UNIVERSITÄT BERN

GSM sniffing

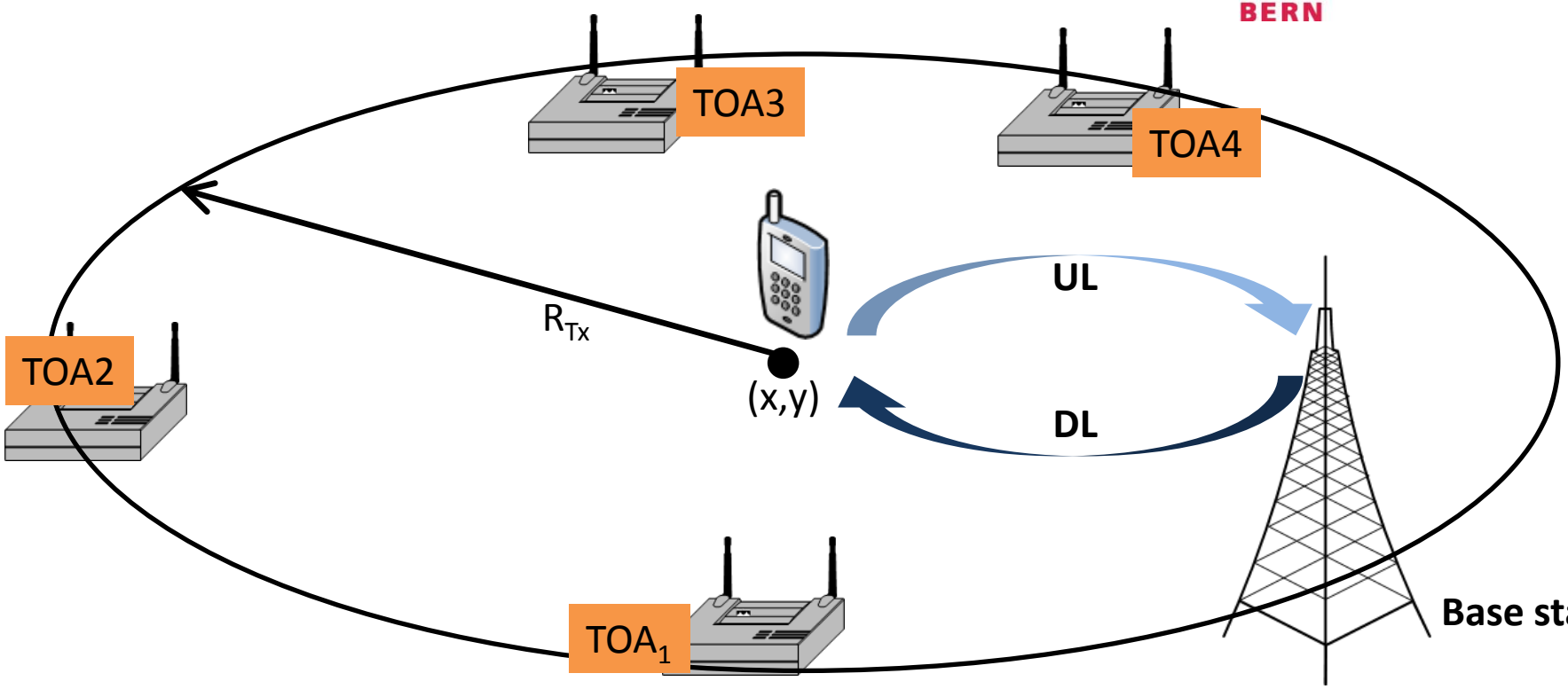
Islam Alyafawi
alyafawi@iam.unibe.ch

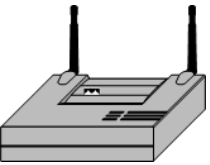
Outline

UNIVERSITÄT BERN

- **In3D guide motivation**
- GSM communication basics
- Sniffing the air:
  - Downlink sniffing
  - Uplink sniffing
- Results
- Challenges/ Future work

Motivation





USRP

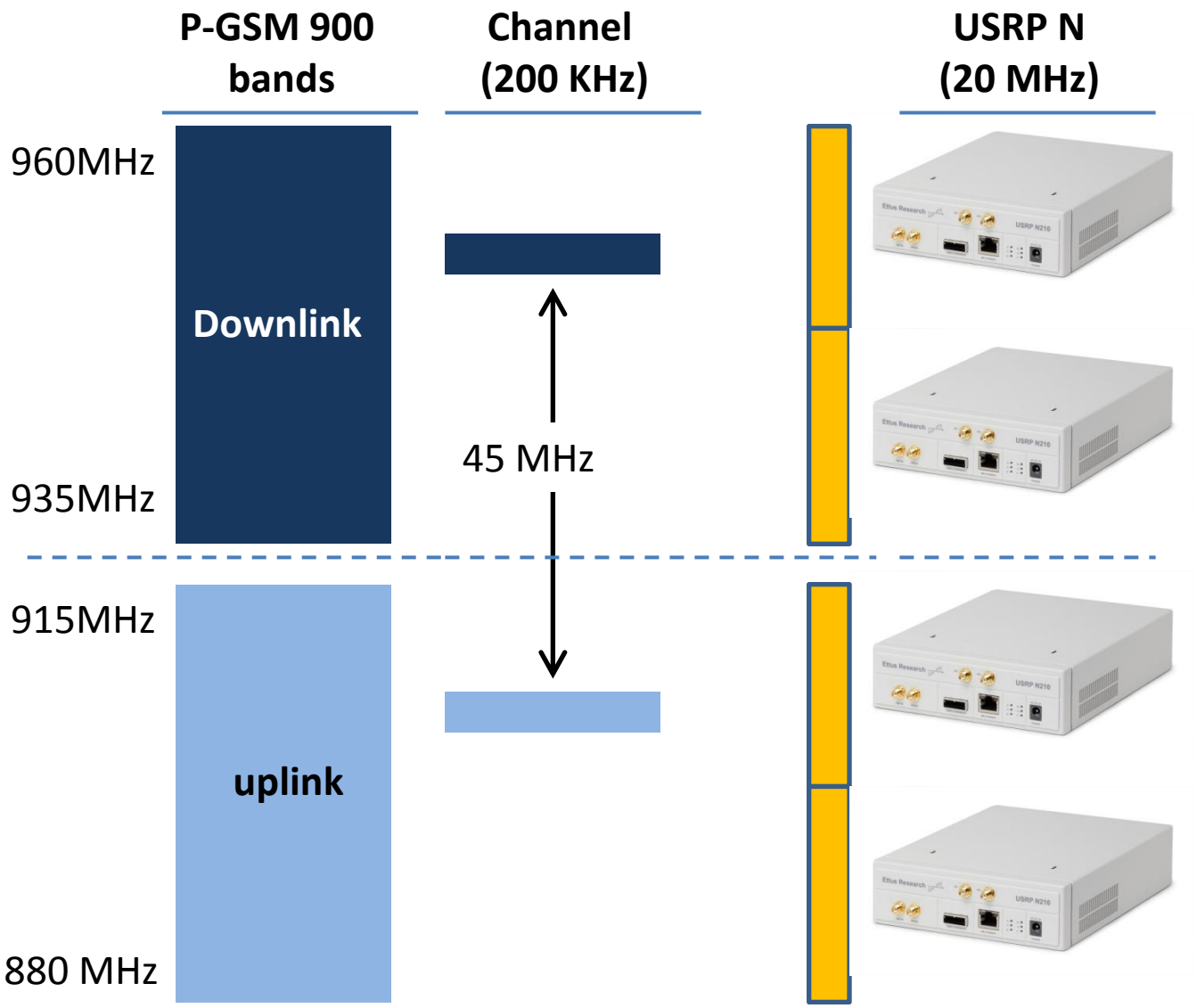
$$(x,y) = f(TOA_1, TOA_2, TOA_3, TOA_4)$$

Outline

UNIVERSITÄT BERN

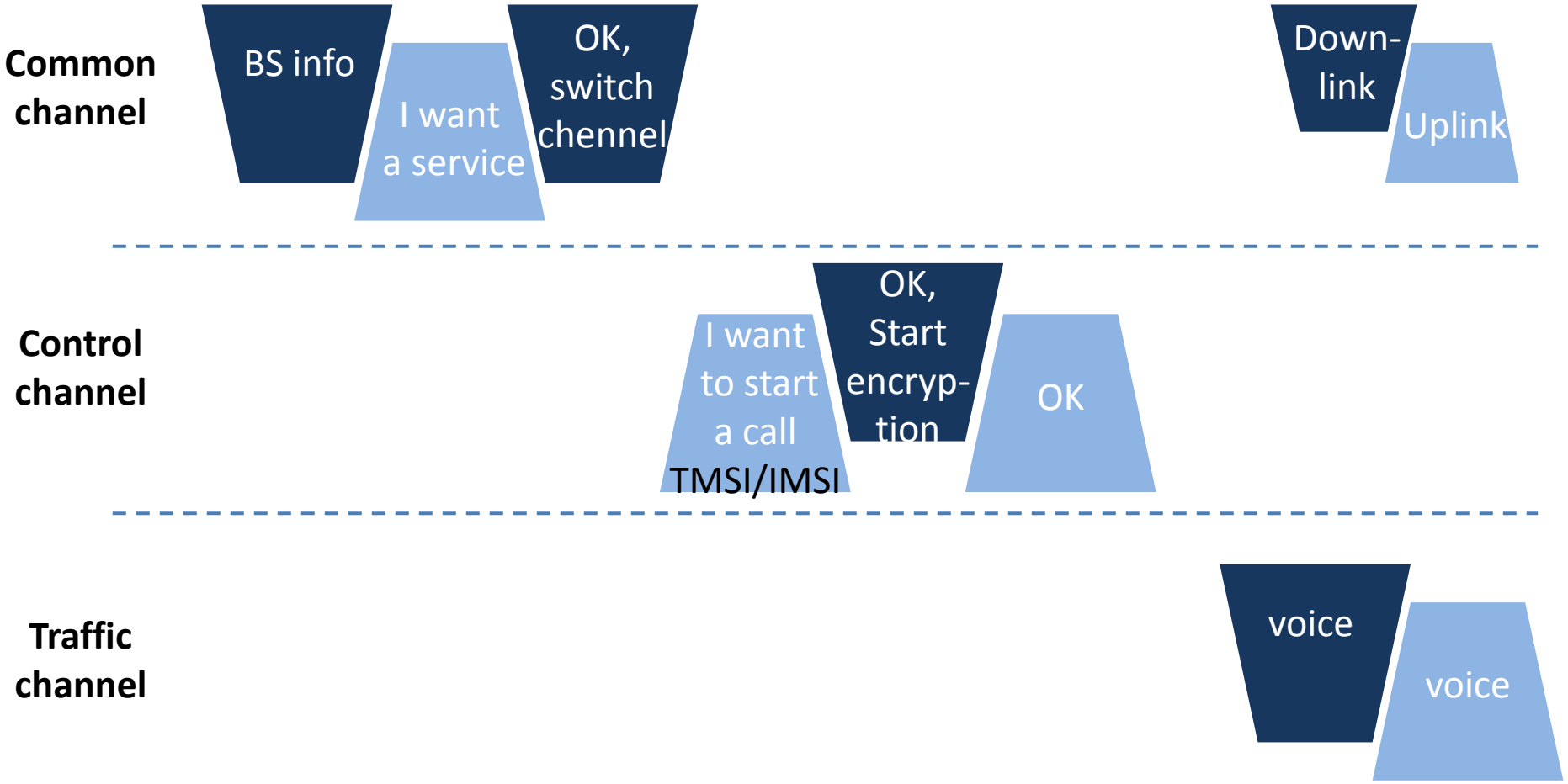
- In3D guide motivation
- **GSM communication basics**
- Sniffing the air:
  - Downlink sniffing
  - Uplink sniffing
- Results
- Challenges/ Future work

GSM Basics -1



USRP N/E Switching betweenDownlink/ uplink

GSM Basics -2



GSM Basics -3

UNIVERSITÄT BERN

Frequency correction Burst (FB)

TB 3	Fixed bits 142	TB 3	GP 8.25

Synchronization Burst (SB)

TB 3	Encrypted bits 39	F 1	Synchronization sequence 64	F 1	Encrypted bits 39	TB 3	GP 8.25

Access Burst (AB)

TB 3	Synchronization sequence 41	Encrypted bits 36	TB 3	GP 68.25

Normal Burst (NB)

TB 3	Encrypted bits 57	F 1	Training sequence 26	F 1	Encrypted bits 57	TB 3	GP 8.25

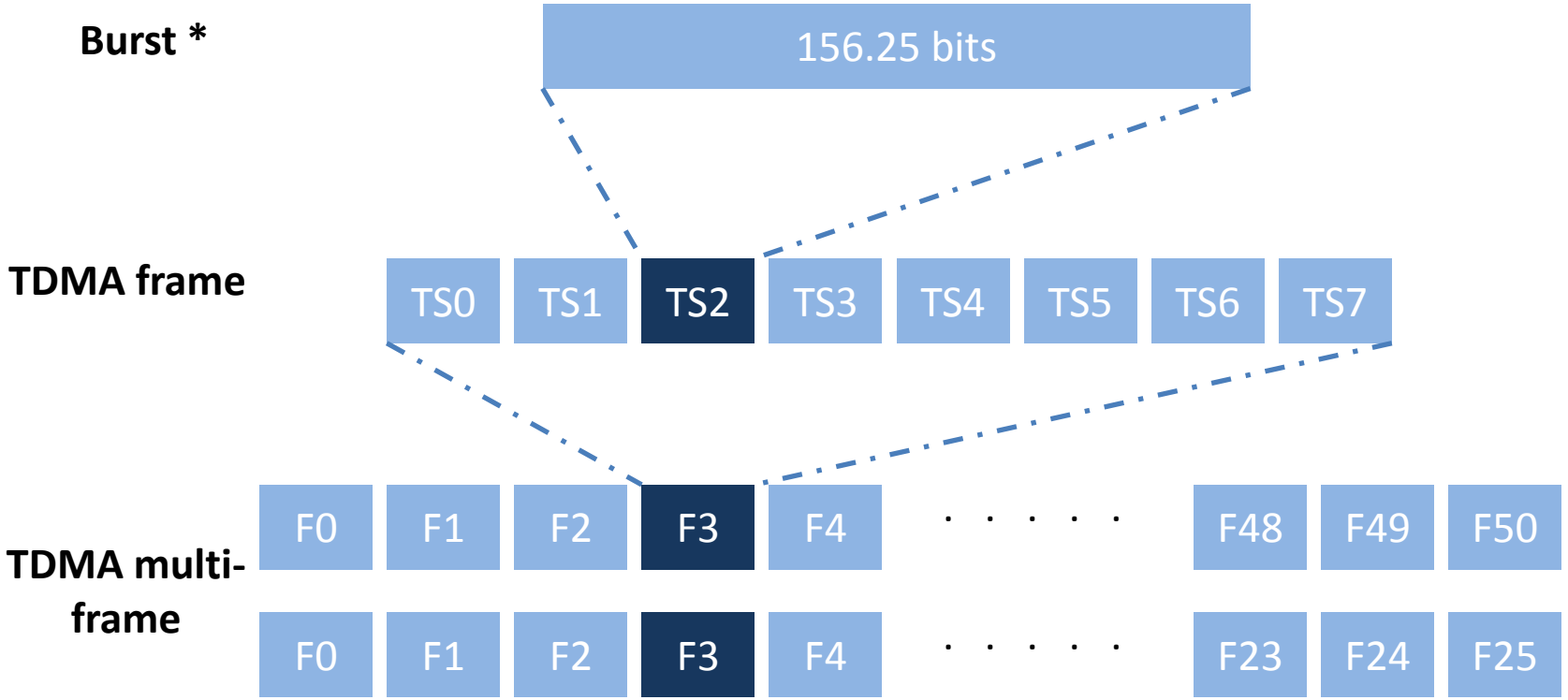
Dummy Burst (DB)

TB 3	Mix bits 58	Training sequence 26	Mix bits 58	TB 3	GP 8.25

Duration
156.25 bits

GSM Basics -4

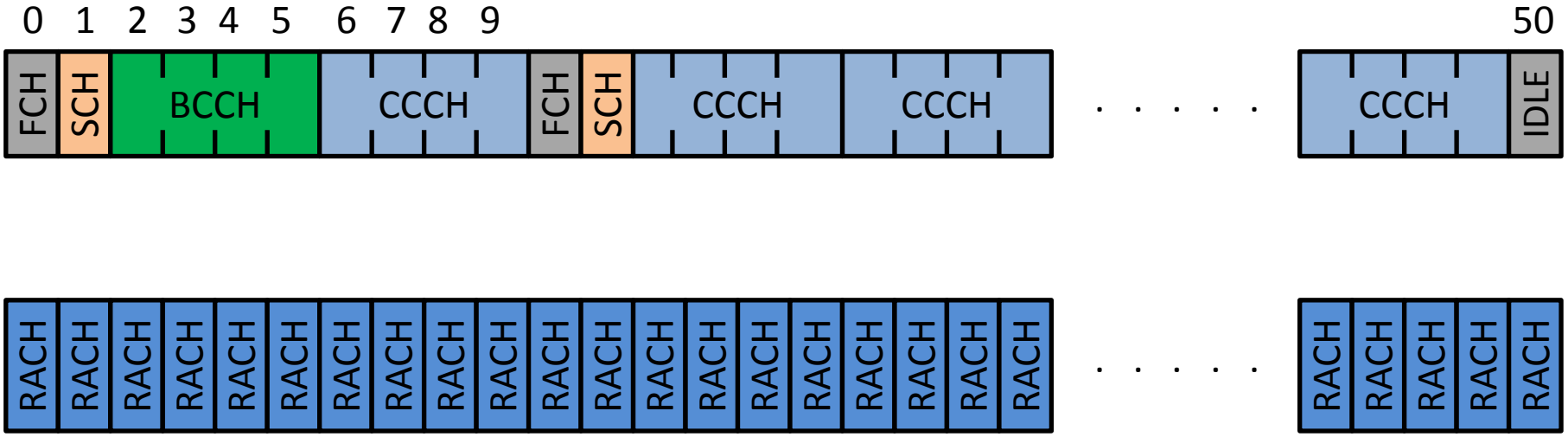
UNIVERSITÄT BERN



GSM Basics -5

UNIVERSITÄT BERN

Downlink/uplink multiframes have predefined pair structure



FCH: Frequency channel
BCCH: Broadcast common channel
RACH: Random access channel

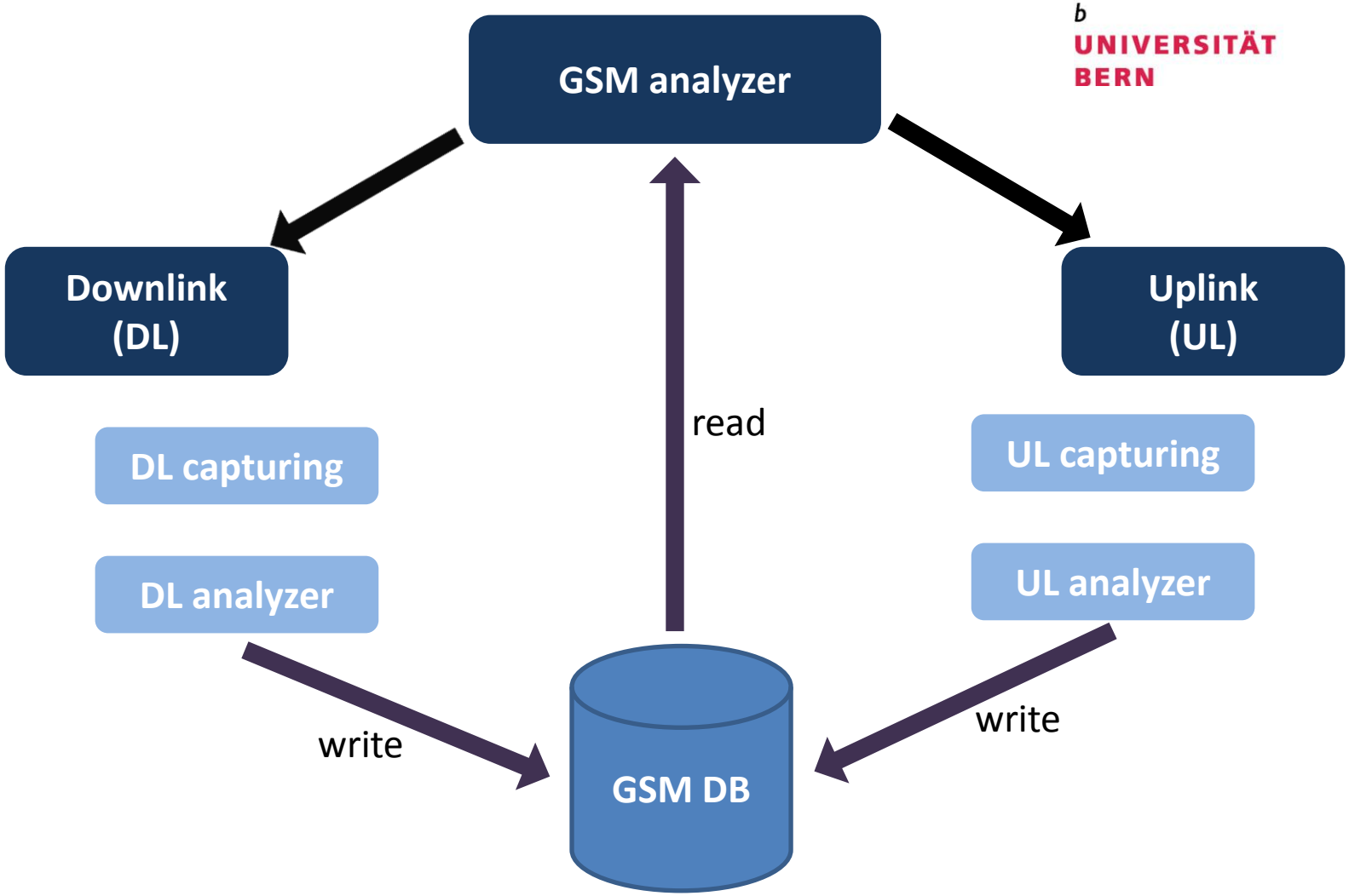
SCH: Synchronization channel
CCCH: Common control channel

Outline

UNIVERSITÄT BERN

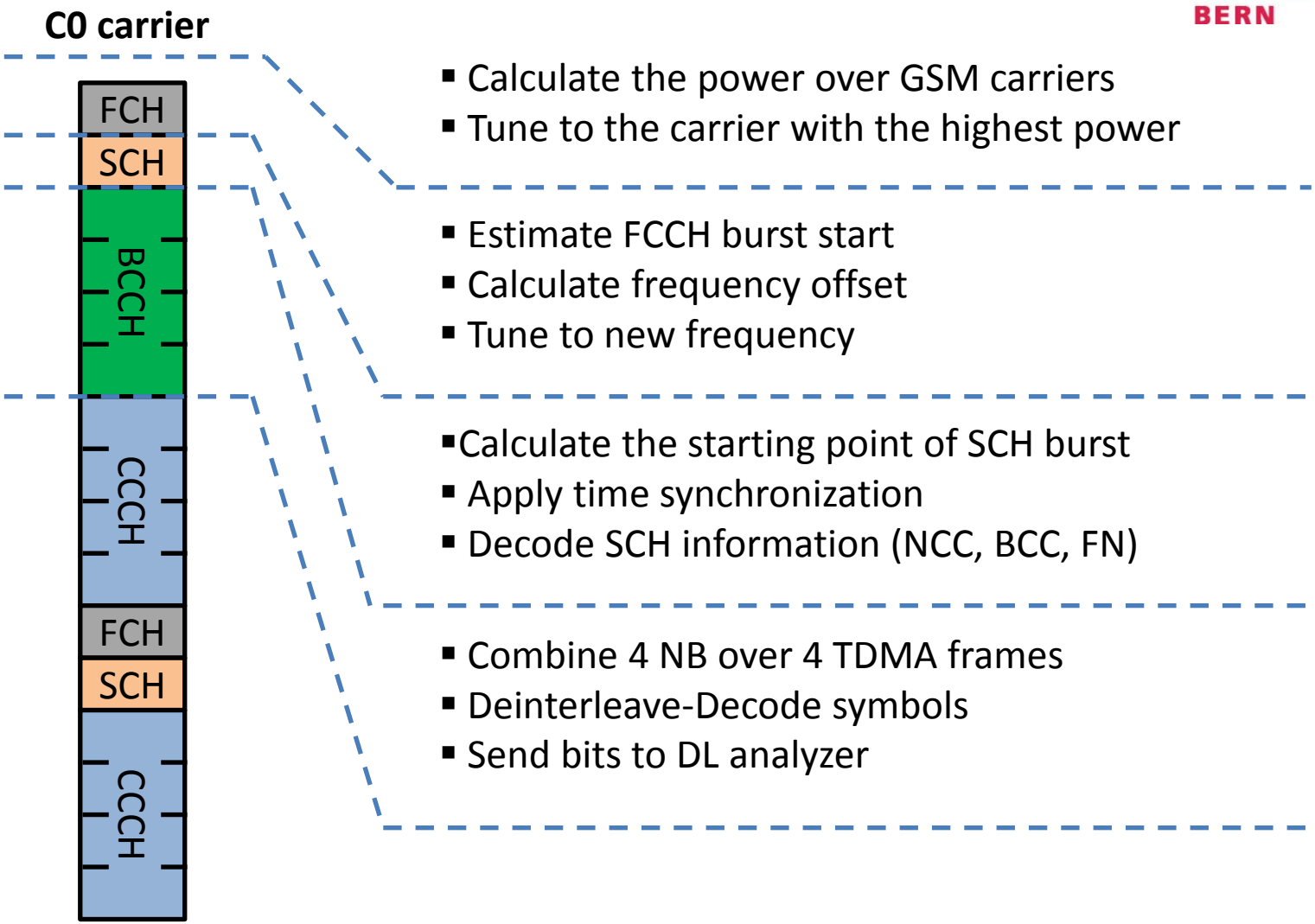
- In3D guide motivation
- GSM communication basics
- **Sniffing the air:**
  - Downlink sniffing
  - Uplink sniffing
- Results
- Challenges/ Future work

Sniffing the air



Downlink sniffing

Synch-based



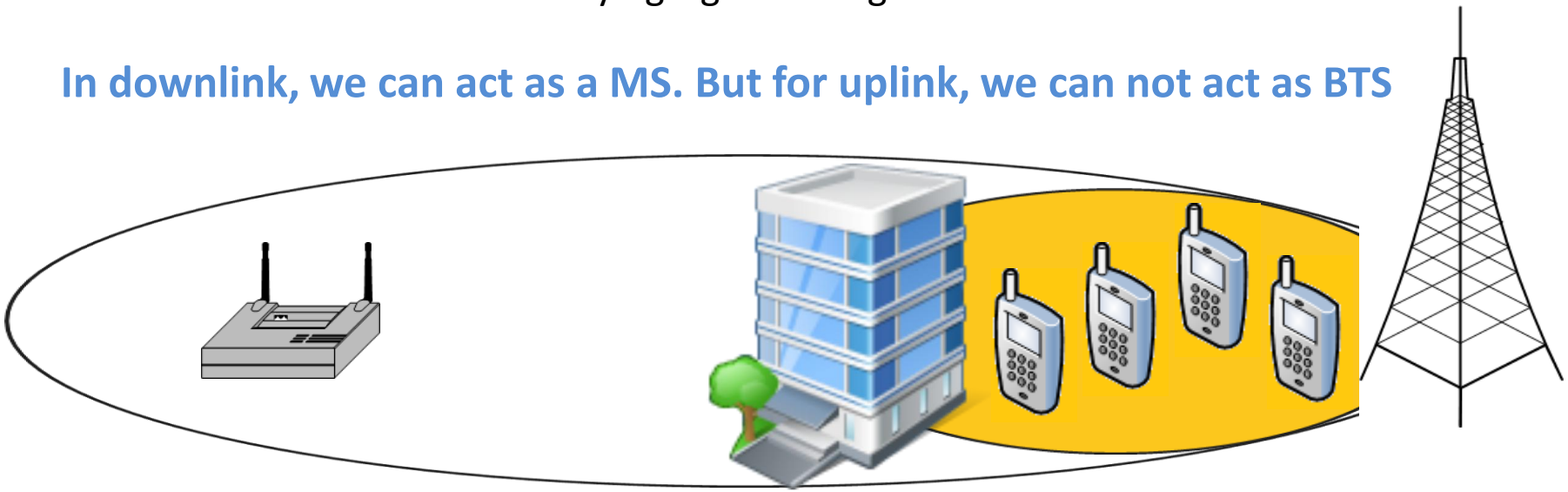
Uplink sniffing - 1

NB-based

UNIVERSITÄT BERN

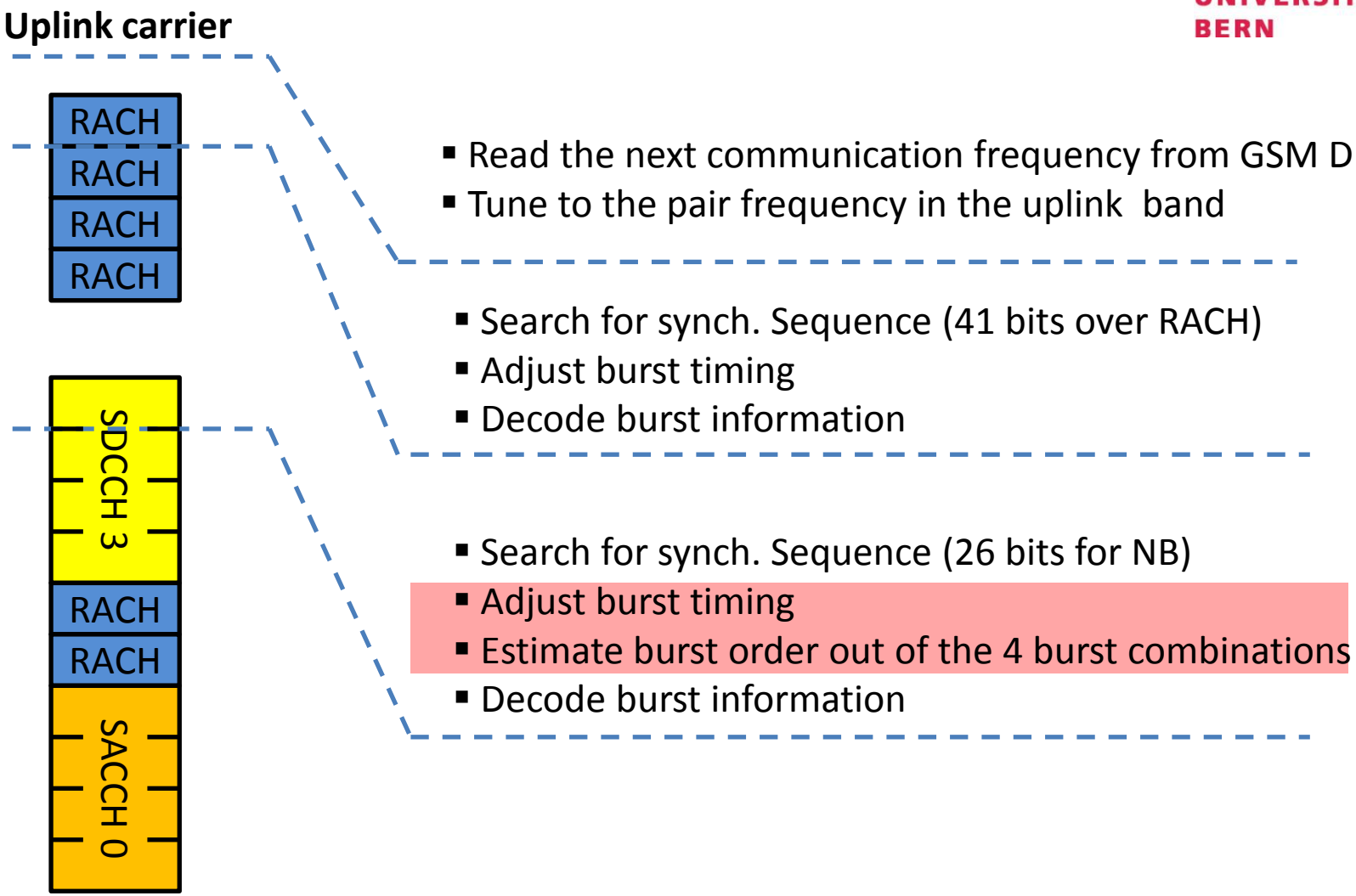
- Handsets are synch w/r/t BTS, but asynch w/r/t USRP
- Uplink Tx power is weaker than Downlink Tx power
- Handsets are typically in a much less radio-visible positions
- Handset move cause varying signal strength

In downlink, we can act as a MS. But for uplink, we can not act as BTS



Uplink sniffing - 1

NB-based



Outline

UNIVERSITÄT BERN

- In3D guide motivation
- GSM communication basics
- Sniffing the air:
  - Downlink sniffing
  - Uplink sniffing
- **Results**
- Challenges/ Future work

Results - 1

Downlink

UNIVERSITÄT BERN

0: 25 001001-- Pseudo Length: 9
1: 06 0------- Direction: From originating site
1: 06 -000---- 0 TransactionID
1: 06 ----0110 Radio Resouce Management
2: 21 00100001 Paging Request Type 1
3: 20 ------00 Page Mode: Normal paging
5: f4 -----100 Type of identity: TMSI/P-TMSI
6: 30 -------- ID(4/even): 30B76B87

Results - 2

Downlink

UNIVERSITÄT BERN

0: 31 001100-- Pseudo Length: 12
1: 06 0------- Direction: From originating site
1: 06 -000---- 0 TransactionID
1: 06 ----0110 Radio Resouce Management
2: 21 00100001 Paging Request Type 1
3: 20 ------00 Page Mode: Normal paging
5: 29 -----001 Type of identity: IMSI
6: 82 -------- ID(7/odd): 228013520137782

Results - 3

Downlink

UNIVERSITÄT BERN

1: 06 ----0110 Radio Resouce Management
2: 3f 0-111111 RRimmediateAssignment
2: 3f -x------ Send sequence number: 0
3: 00 ------00 Page Mode: Normal paging
3: 00 --0----- Downlink assign to MS: No meaning
3: 00 ---0---- This messages assigns a dedicated mode resource
4: 48 -----000 Timeslot number: 0
4: 48 01001--- Channel Description: SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8), SC1
5: 70 011----- Training seq. code : 3
5: 70 ---1---- HoppingChannel
6: 3b ..... Mobile Allocation Index Offset (MAIO) 0
6: 3b --111011 Hopping Seq. Number: 59
7: 24 ---xxxxx Random Reference : 4
10: 02 --xxxxxx Timing advance value: 2

Results - 4

Synch-based

UNIVERSITÄT BERN

Message type	N messages (USRP E110 / USRP N210)	Ratio between 2 USRP N210
Paging request type 1	2.5 %	98.5 %
Paging request type 2	2.0 %	99.9 %
Paging request type 3	2.1 %	96.6 %
RR System Info1	1.0 %	98.9 %
RR System Info3C	1.8 %	98.4 %
RR System Info4	1.6 %	99.2 %
RR immediate Assignment	1.6 %	98.6 %

Results - 4

NB-based

UNIVERSITÄT BERN

Message type	N messages (USRP E110 / USRP N210)	Ratio between 2 USRP N210
Paging request type 1	12.2 %	98.0 %
Paging request type 2	24.98 %	98.5 %
Paging request type 3	14.8 %	98.3 %
RR System Info1	15.8 %	99.1 %
RR System Info3C	14.8 %	98.0 %
RR System Info4	14.8 %	97.7 %
RR immediate Assignment	12.4 %	97.6 %

Results - 4

UNIVERSITÄT BERN

Message type	NB-based/ Synch-based
Paging request type 1	110.6 %
Paging request type 2	193.0 %
Paging request type 3	339.0 %
RR System Info1	113.3 %
RR System Info3C	111.9 %
RR System Info4	111.9 %
RR immediate Assignment	135.3 %

Results - 3

Uplink- RACH

UNIVERSITÄT BERN

Message type	Any BSIC	Unique BSIC
	Number of messages/ 30 min	Number of messages/ 8 hours
Answer to paging	136	162
Originating call	66	47
Location updating	23	17
Call re-establishment	72	60
Originating speech call from dual-rate mobile station	23	16
Emergency call	72	67

Outline

UNIVERSITÄT BERN

- In3D guide motivation
- GSM communication basics
- Sniffing the air:
  - Downlink sniffing
  - Uplink sniffing
- Results
- **Challenges/ Future work**

Challenges/ Future work

UNIVERSITÄT BERN

- Fast switching between downlink/uplink frequencies
- Code perfoemance to avoid „ data overflow“ using USRP E110
- Observations for user Identification – few procedures carry ID – not so frequent – encryption

- Capturing Normal bursts in uplink channels
- Updating uplink receiver with burst-type recognition scheme
- Updating DL/UL analyzers with required messages
- Parameters optimization in NB-based code
- Toward GSM-1800

UNIVERSITÄT
BERN

Question