Catching and Understanding GSM signals

Master Thesis

Fabian van den Broek

Radboud University Nijmegen

30 March 2010

Some Numbers

Some Numbers

- $ 600 Billion

Some Numbers

- $ 600 Billion
- 90% of population has coverage

Some Numbers

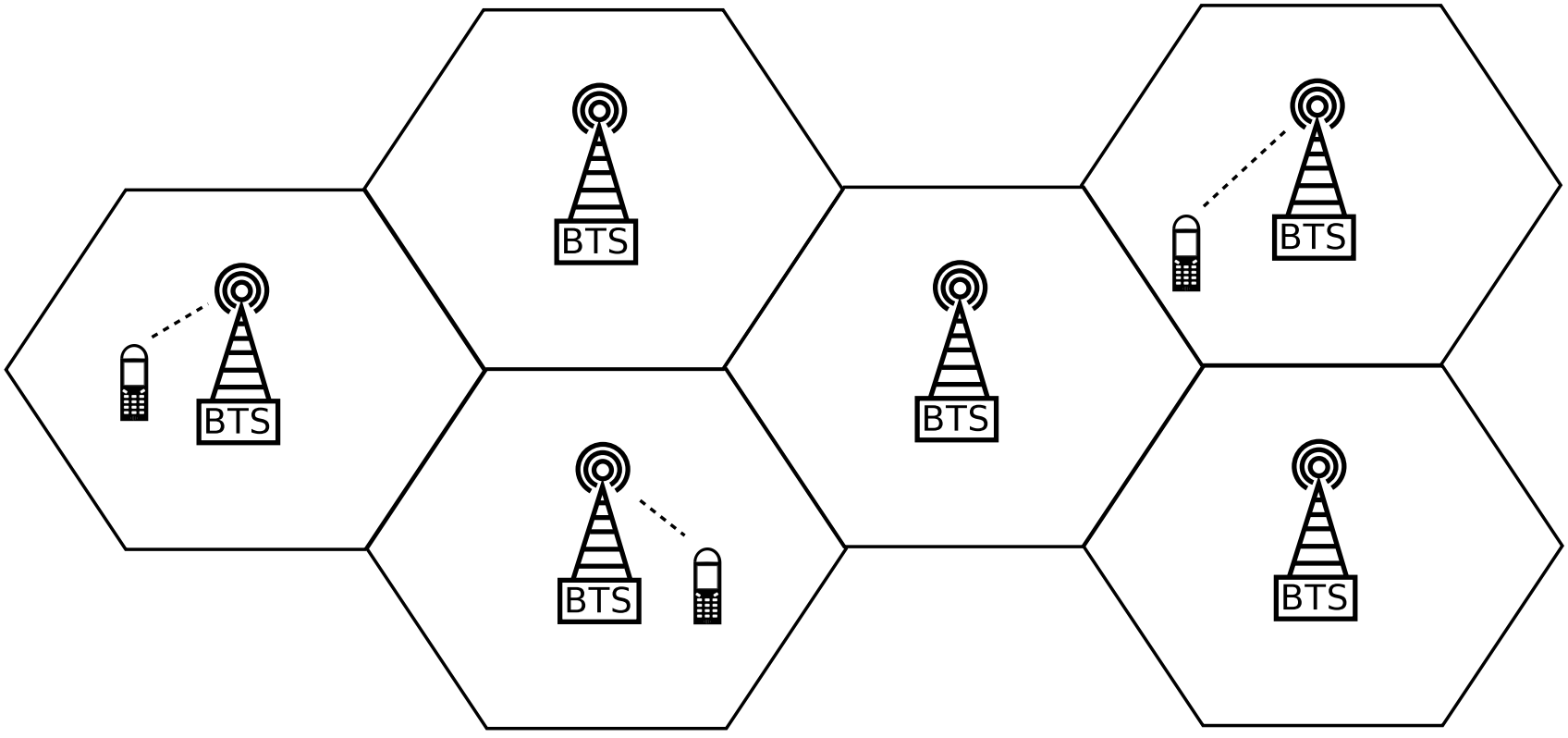
- $ 600 Billion
- 90% of population has coverage
- 4.1 billion mobile users

Some Numbers

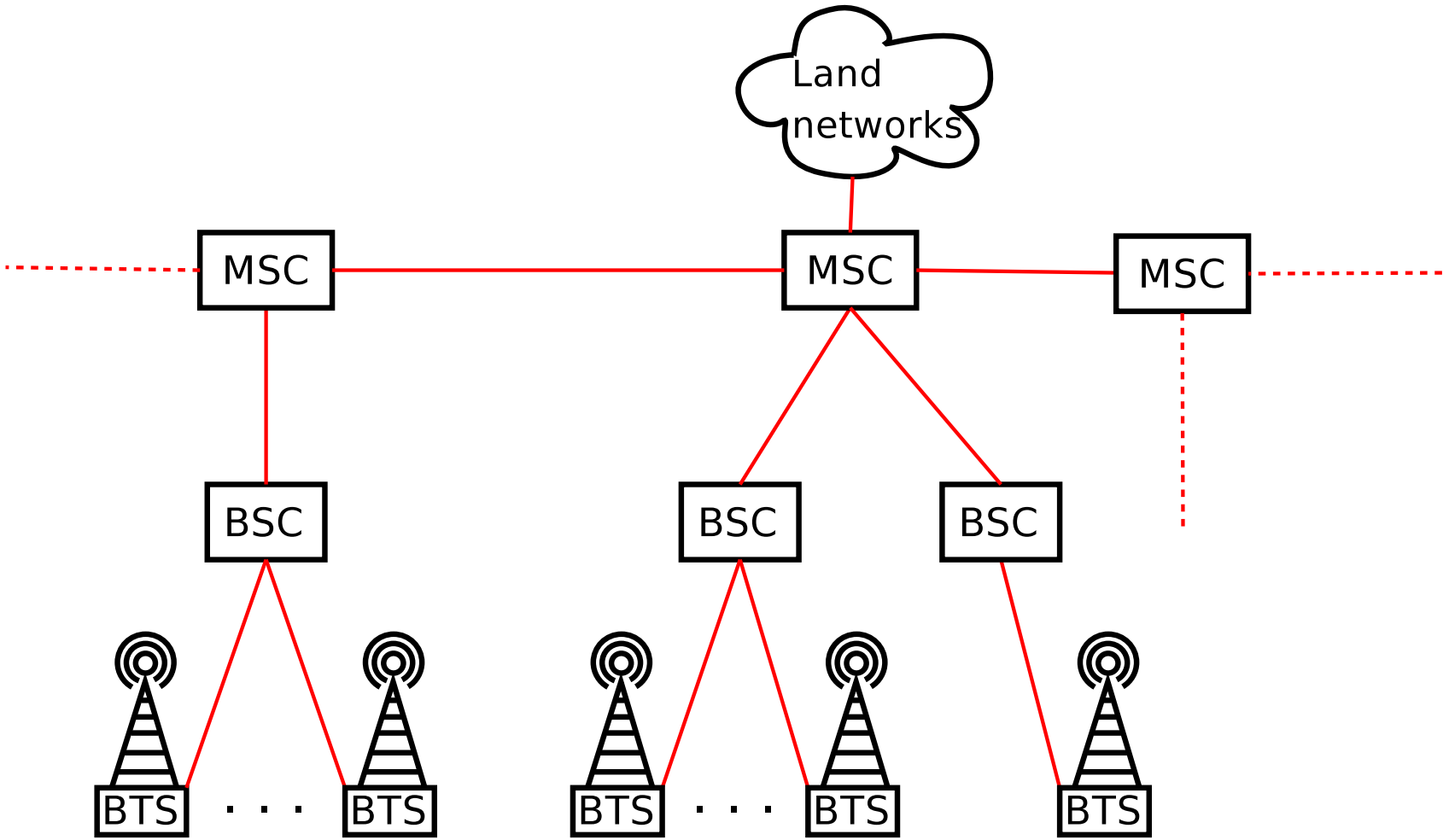
- $ 600 Billion
- 90% of population has coverage
- 4.1 billion mobile users

But has GSM been properly tested?

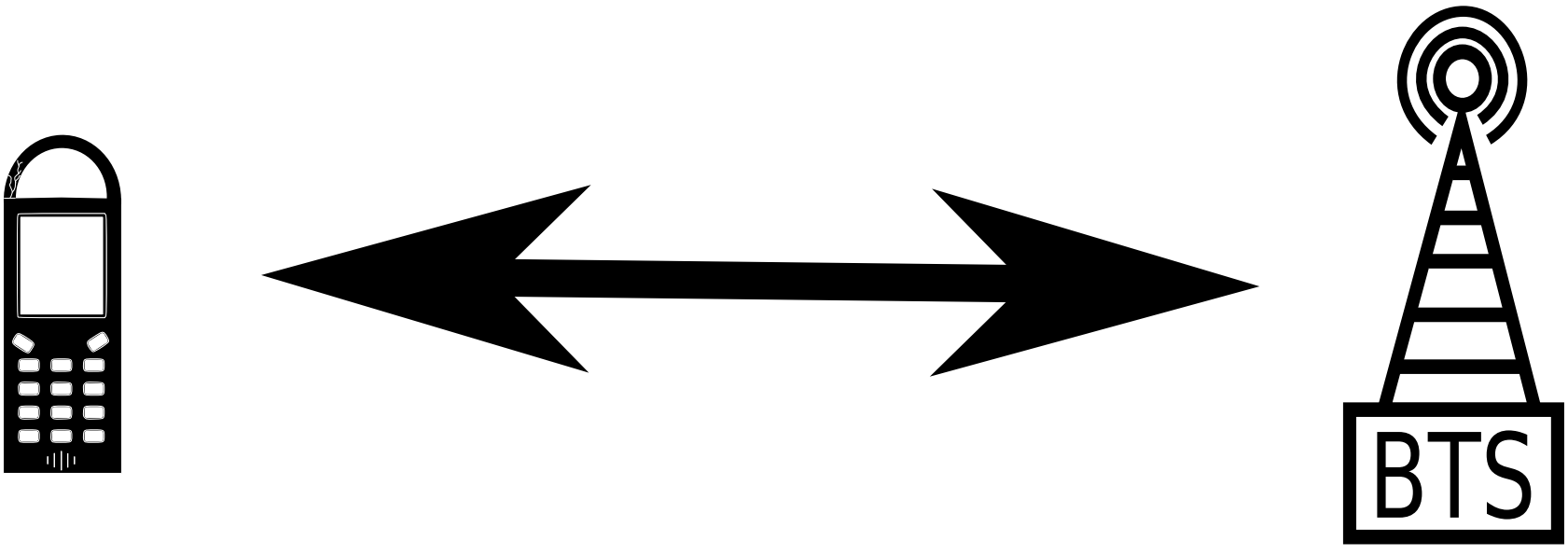
Cellular technology



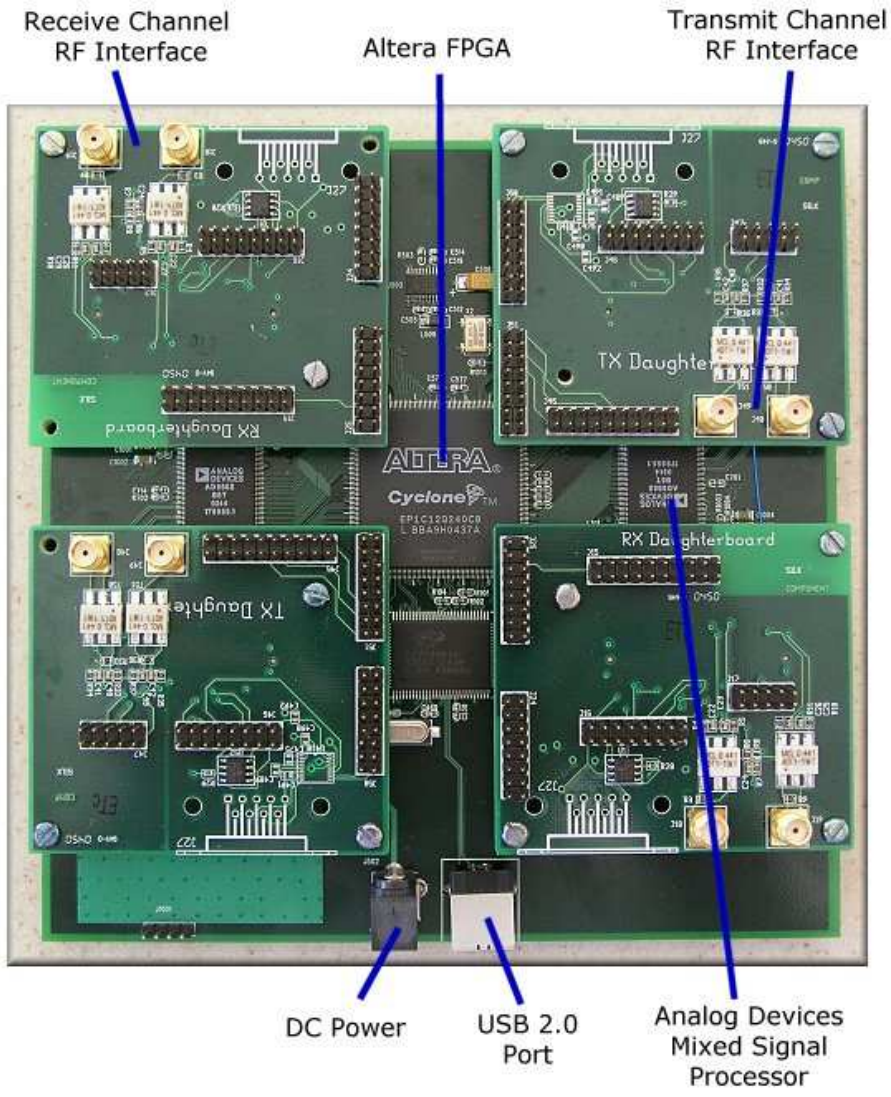
GSM system overview



The Um interface



Software Defined Radio



Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?

Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?

Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?

Software Defined Radio

- USRP
- Gnu Radio
- Air Probe

Have these new SDR products made GSM less secure?

and then....

de Volkskrant

GSM-encryptie gekraakt

The New York Times

Cellphone Encryption Code Is Divulged

cnet news

Cracking GSM phone crypto via distributed computing

PHYSORG.COM

SCIENCE : PHYSICS : TECH : NANO : NEWS

Guide to breaking cell phone security revealed

PCWorld

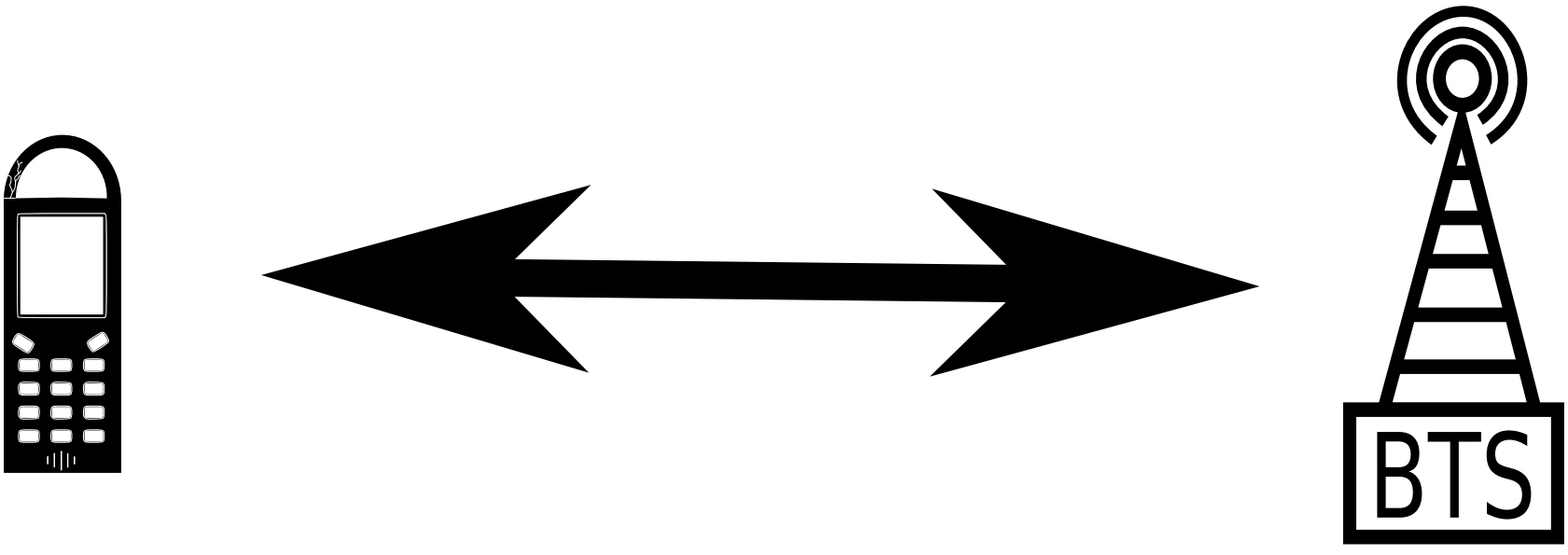
Hackers Show It's Easy to Snoop on a GSM Call

The Register®

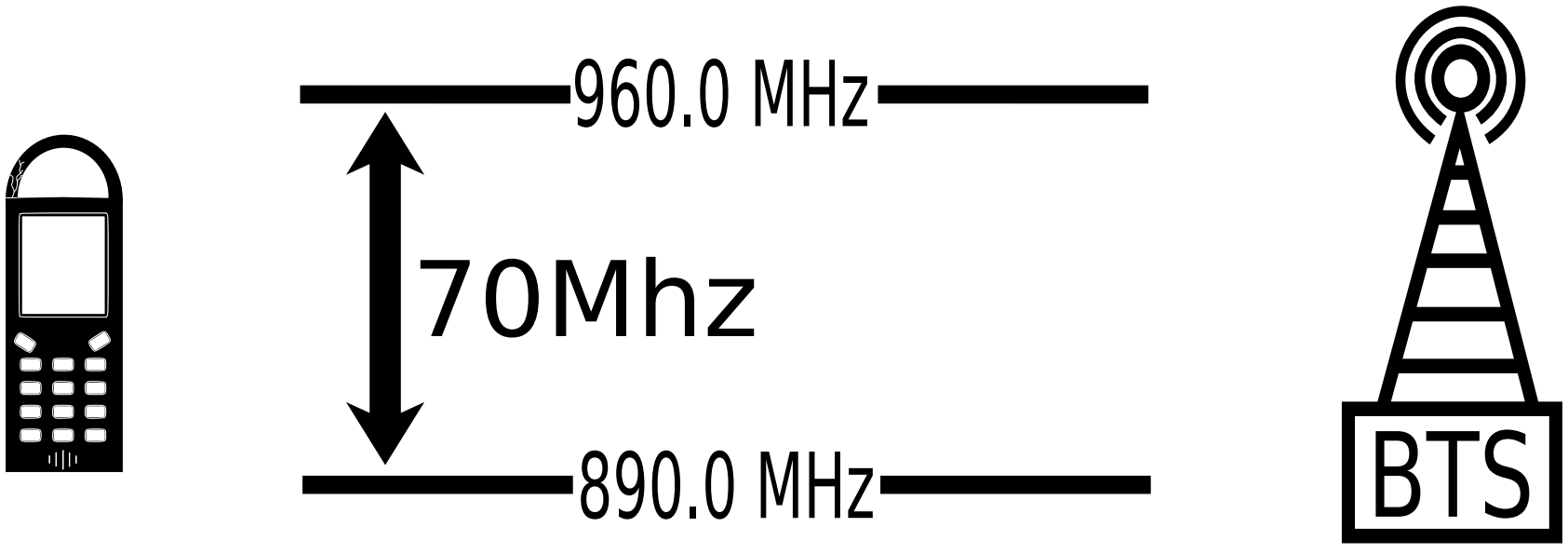
Secret code protecting cellphone calls set loose

Universal phone snooping moves forward

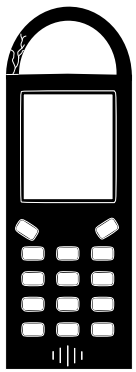
The Um interface

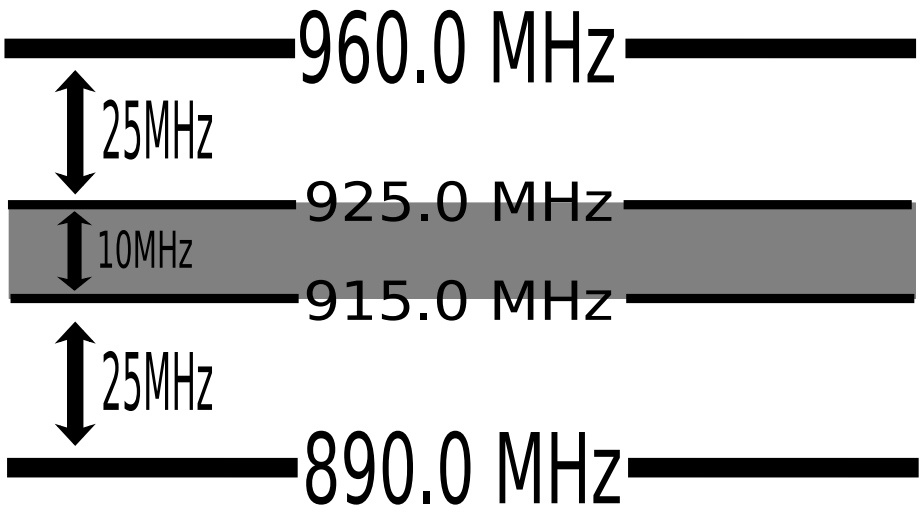


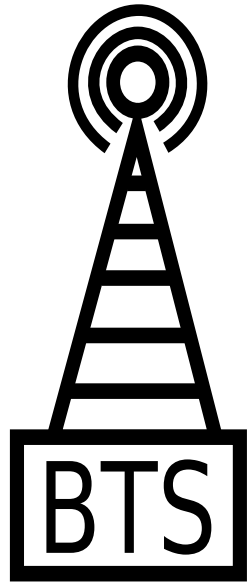
Frequency band (GSM900)



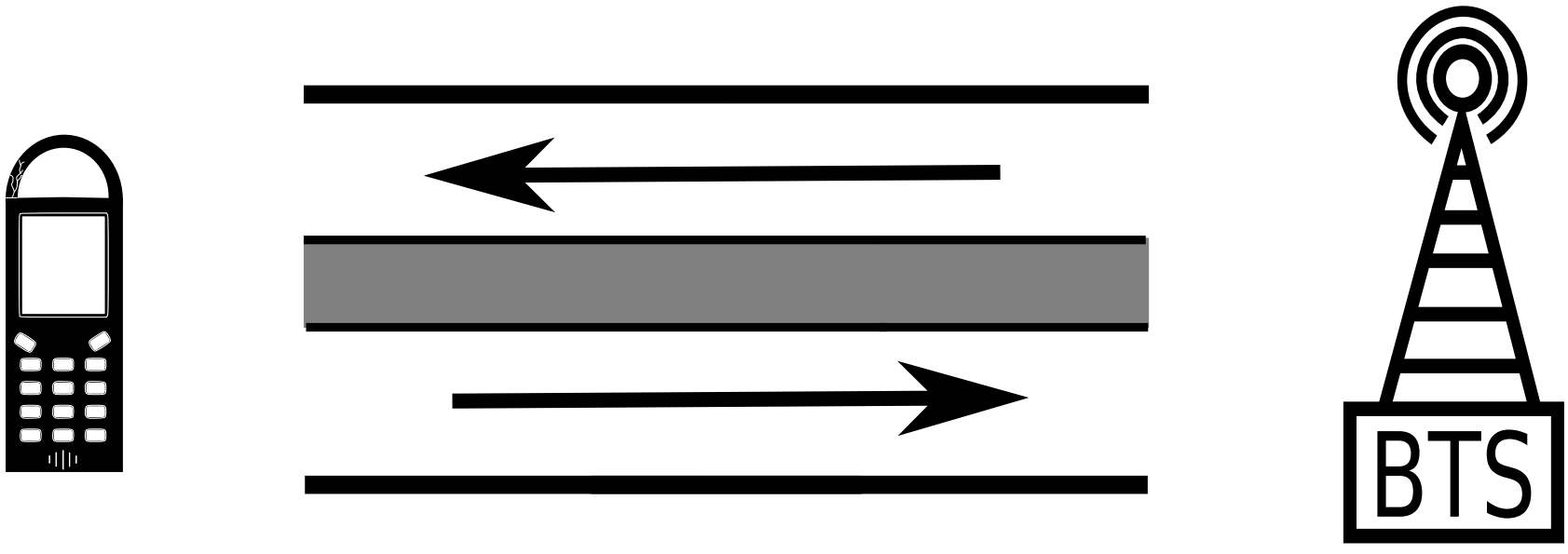
Frequency band (II)



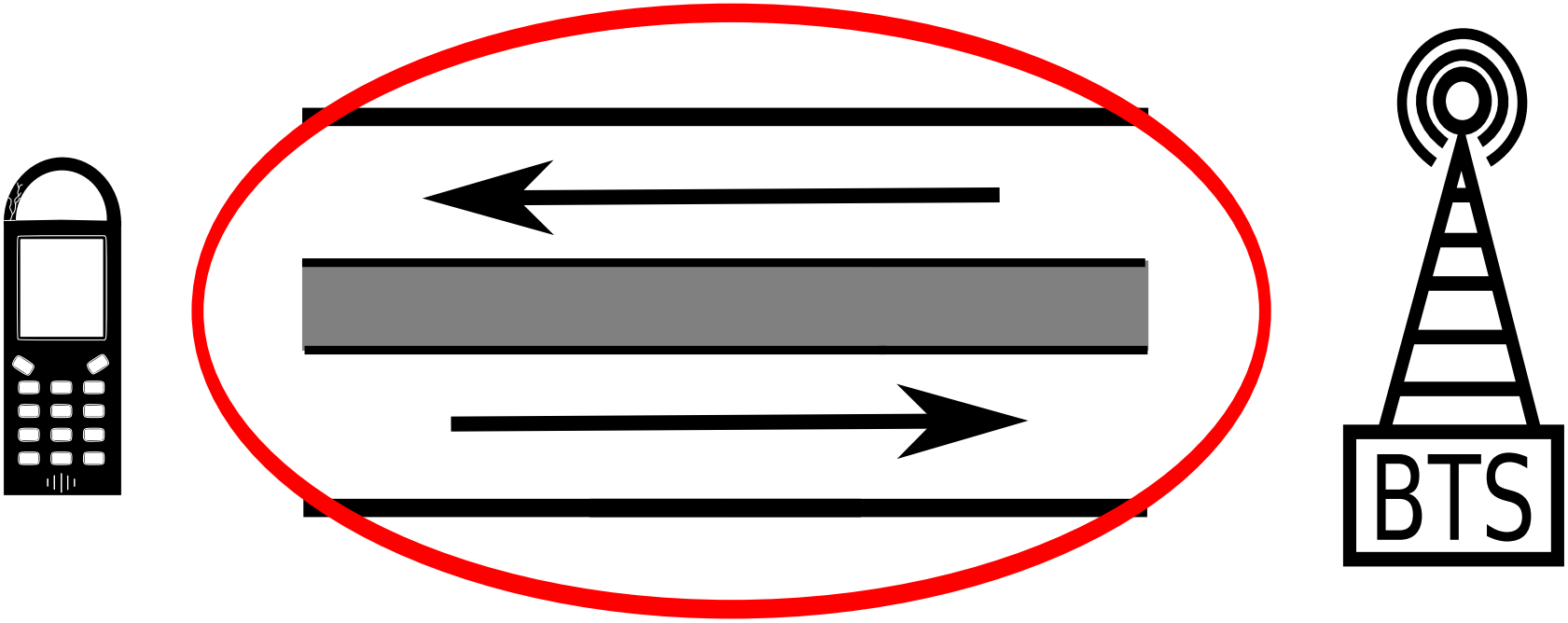




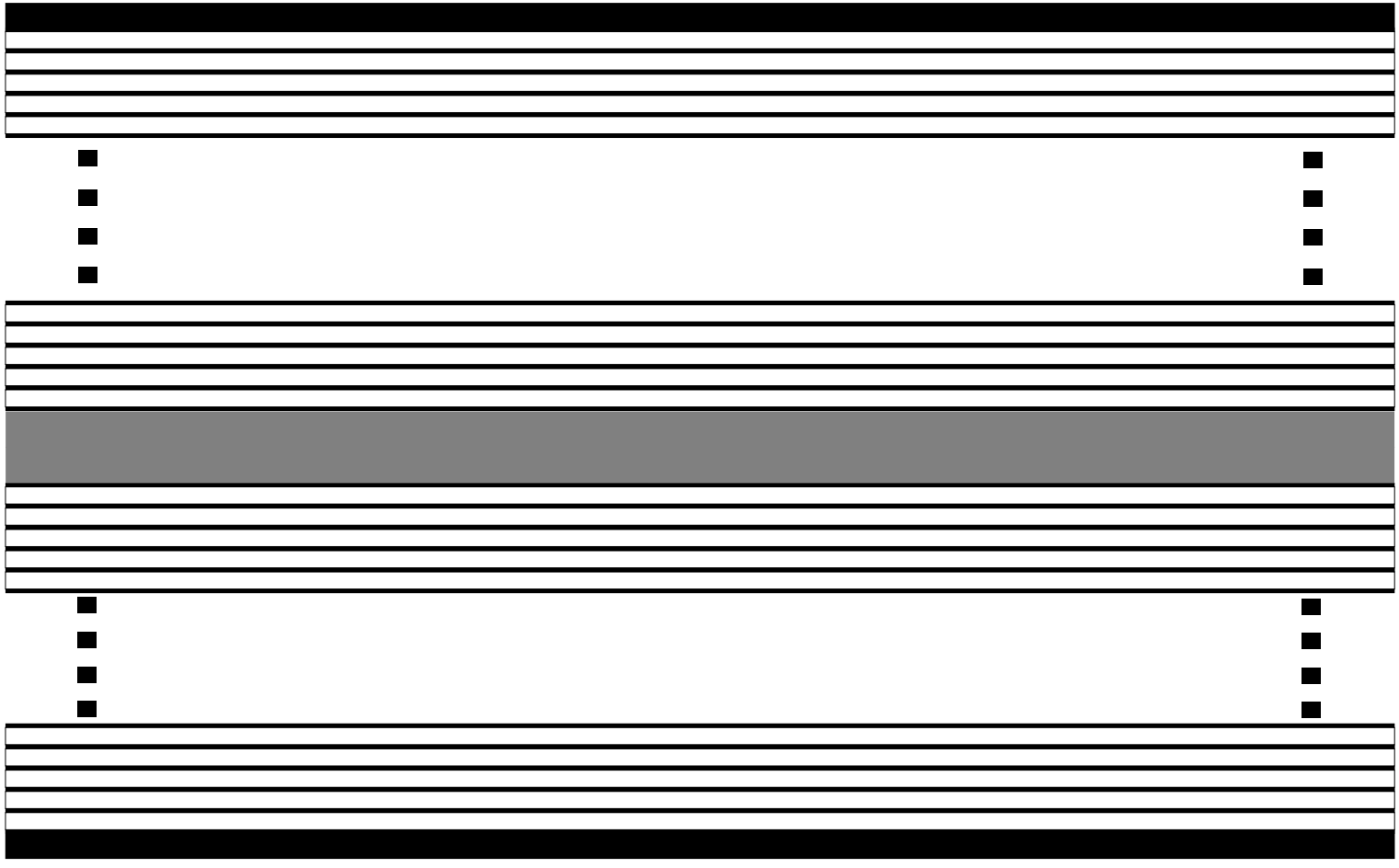
Frequency band (III)



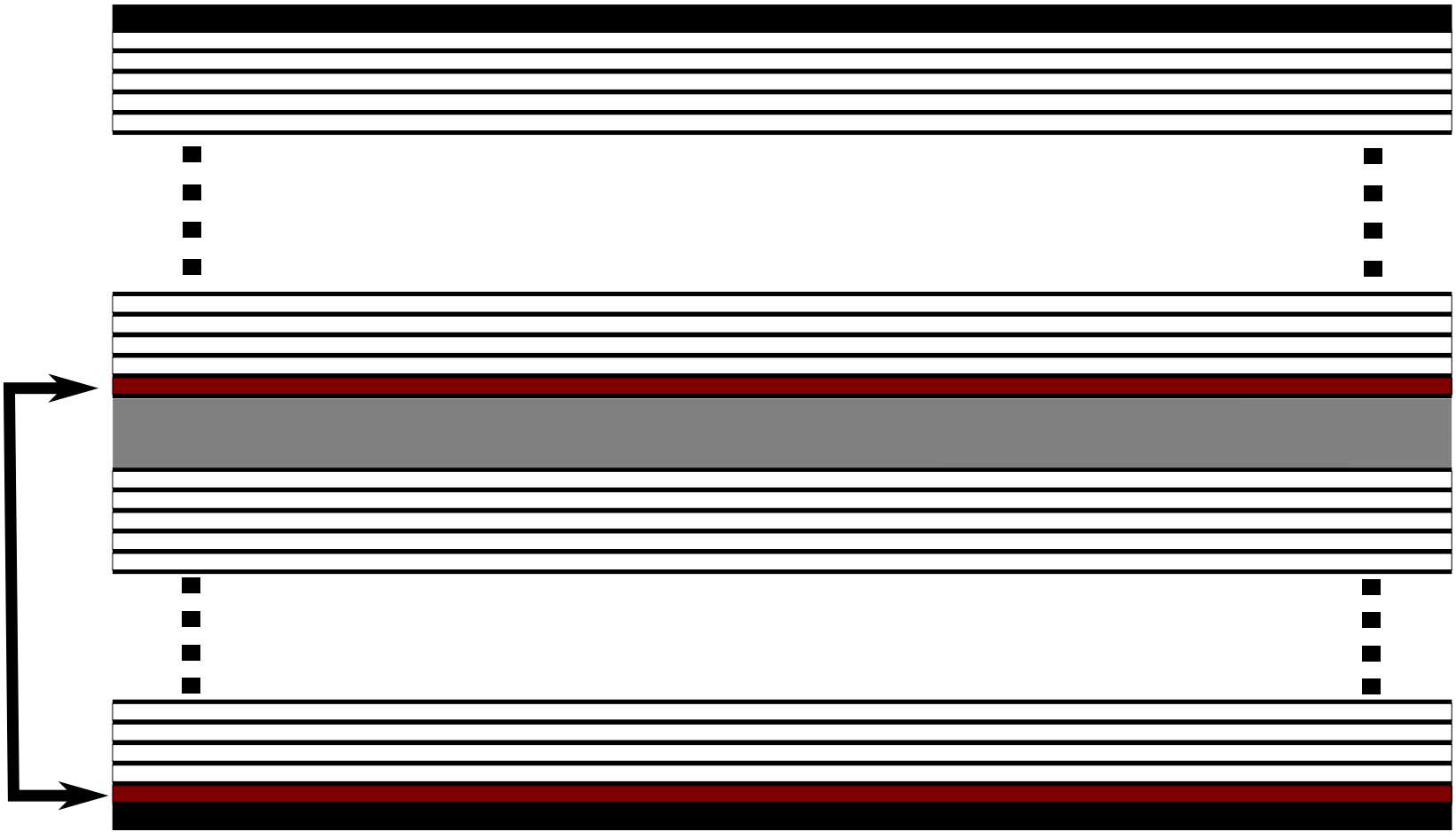
Frequency band (III)



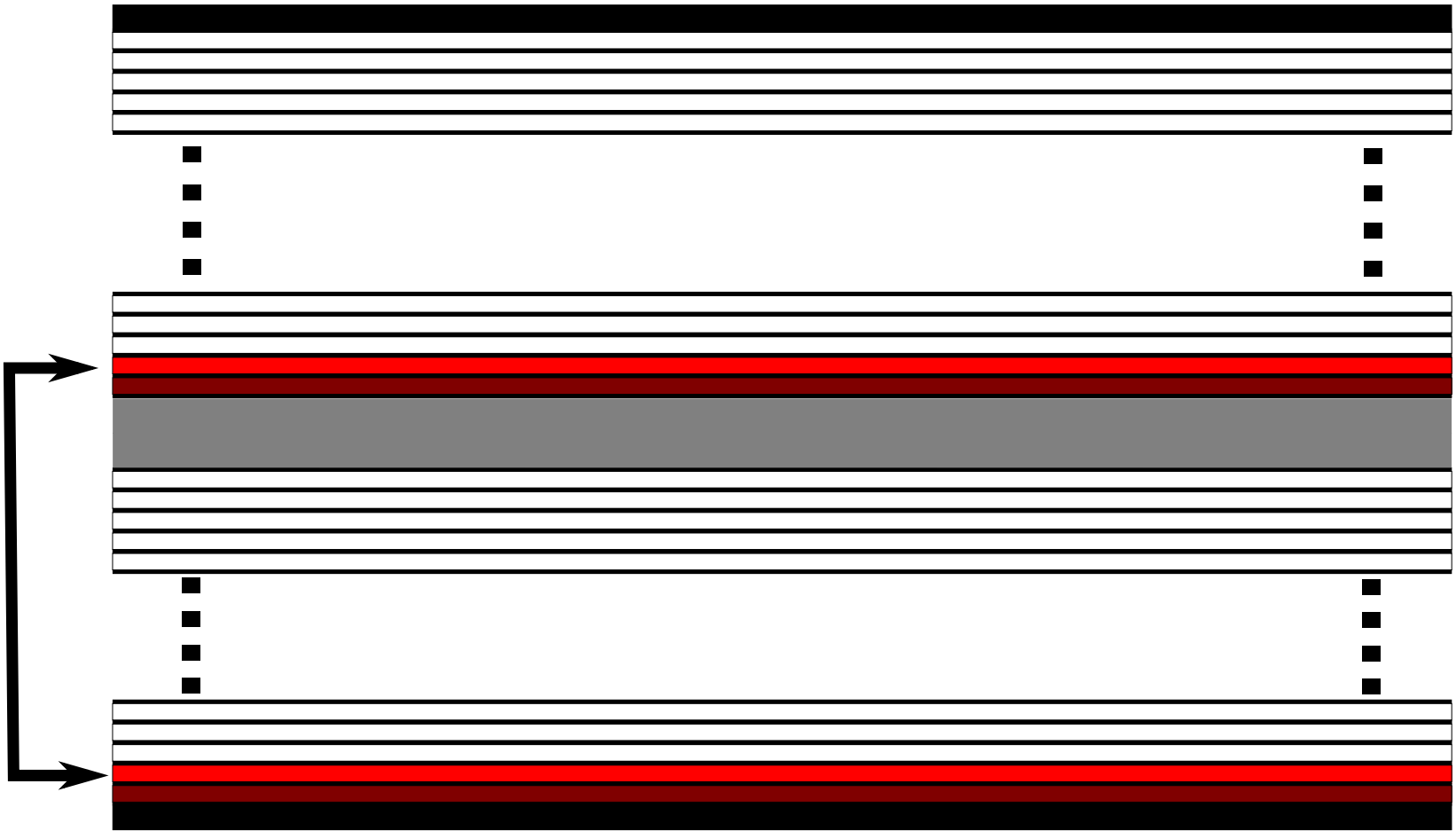
Frequency division



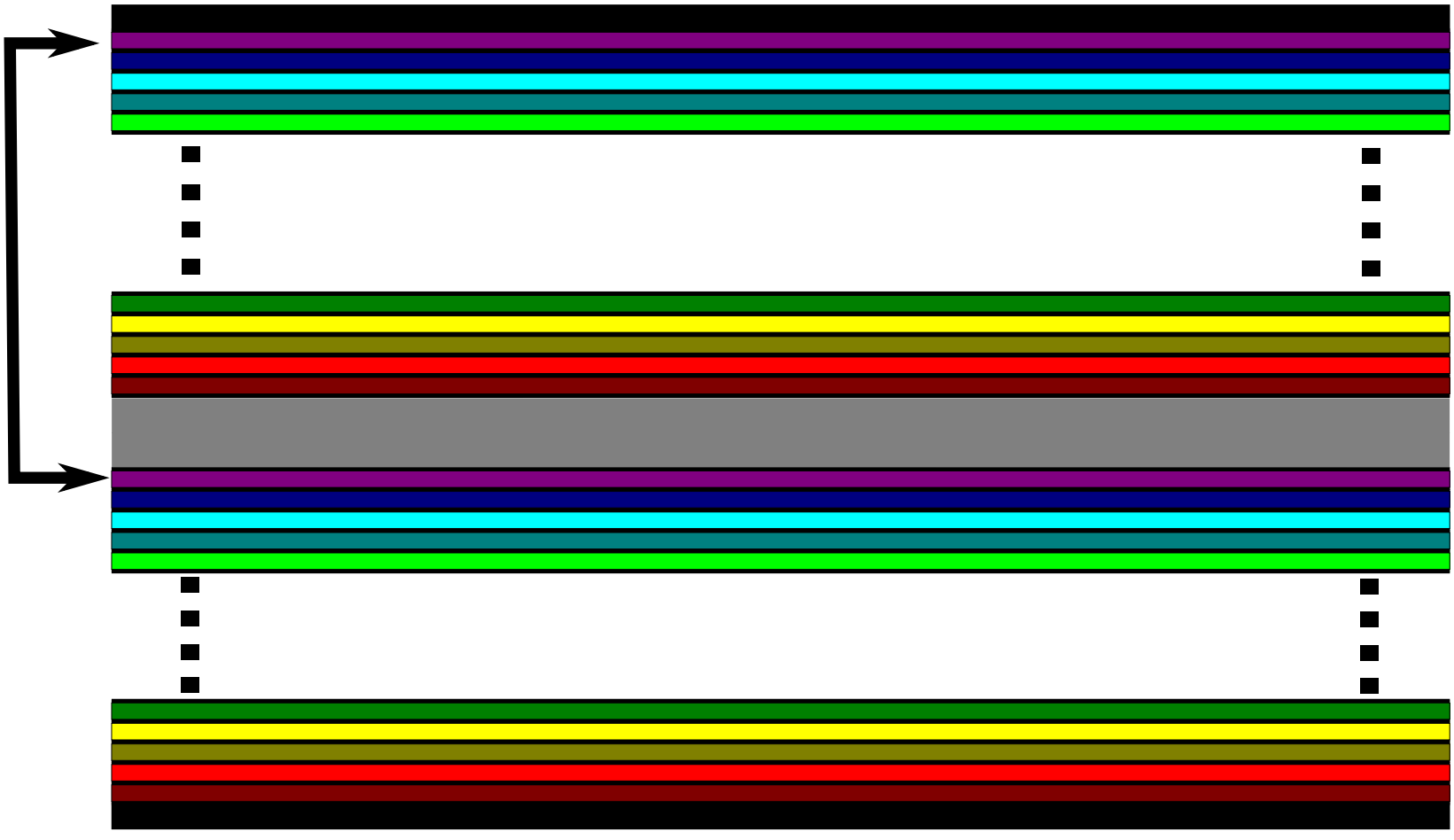
Combined up and down link frequency



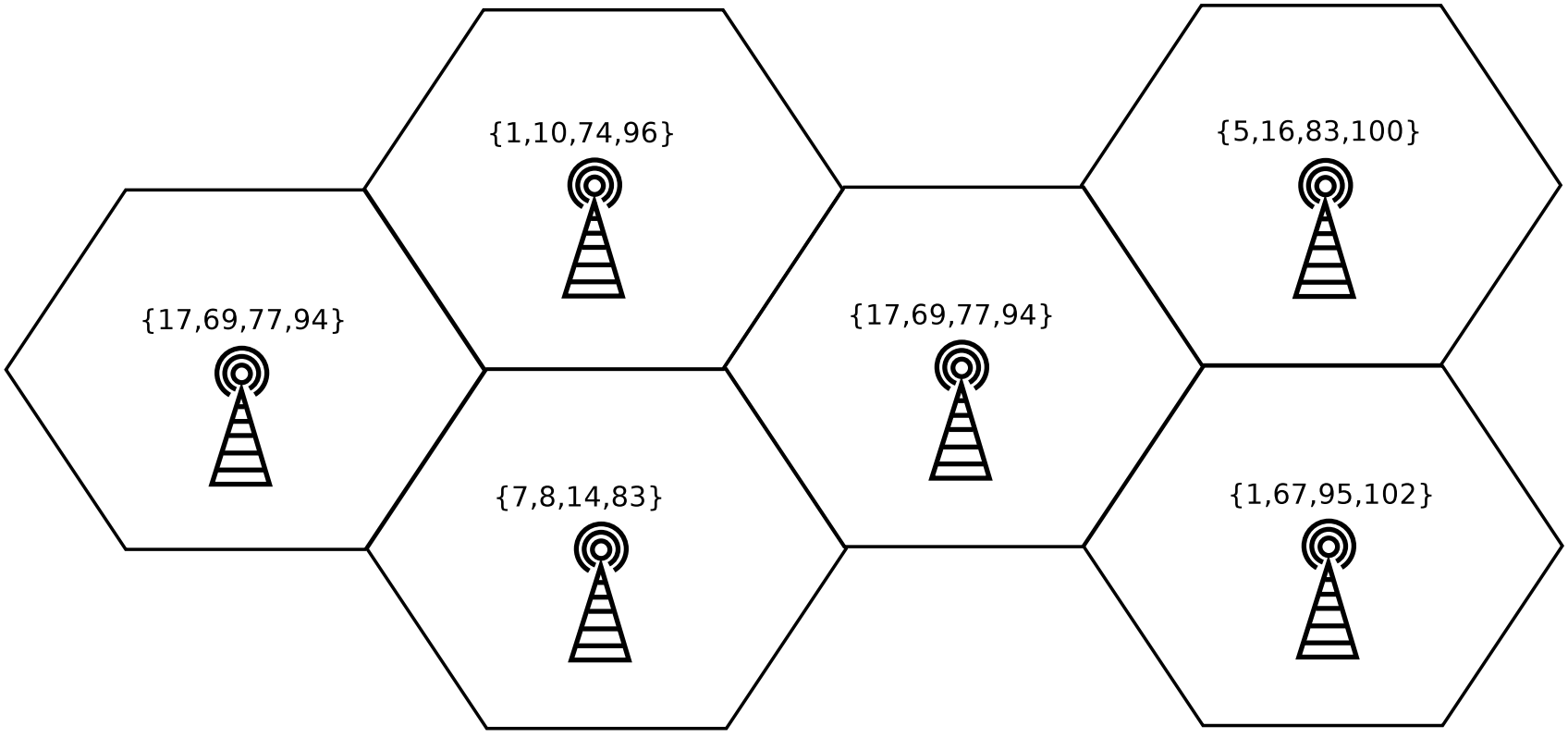
Combined up and down link frequency



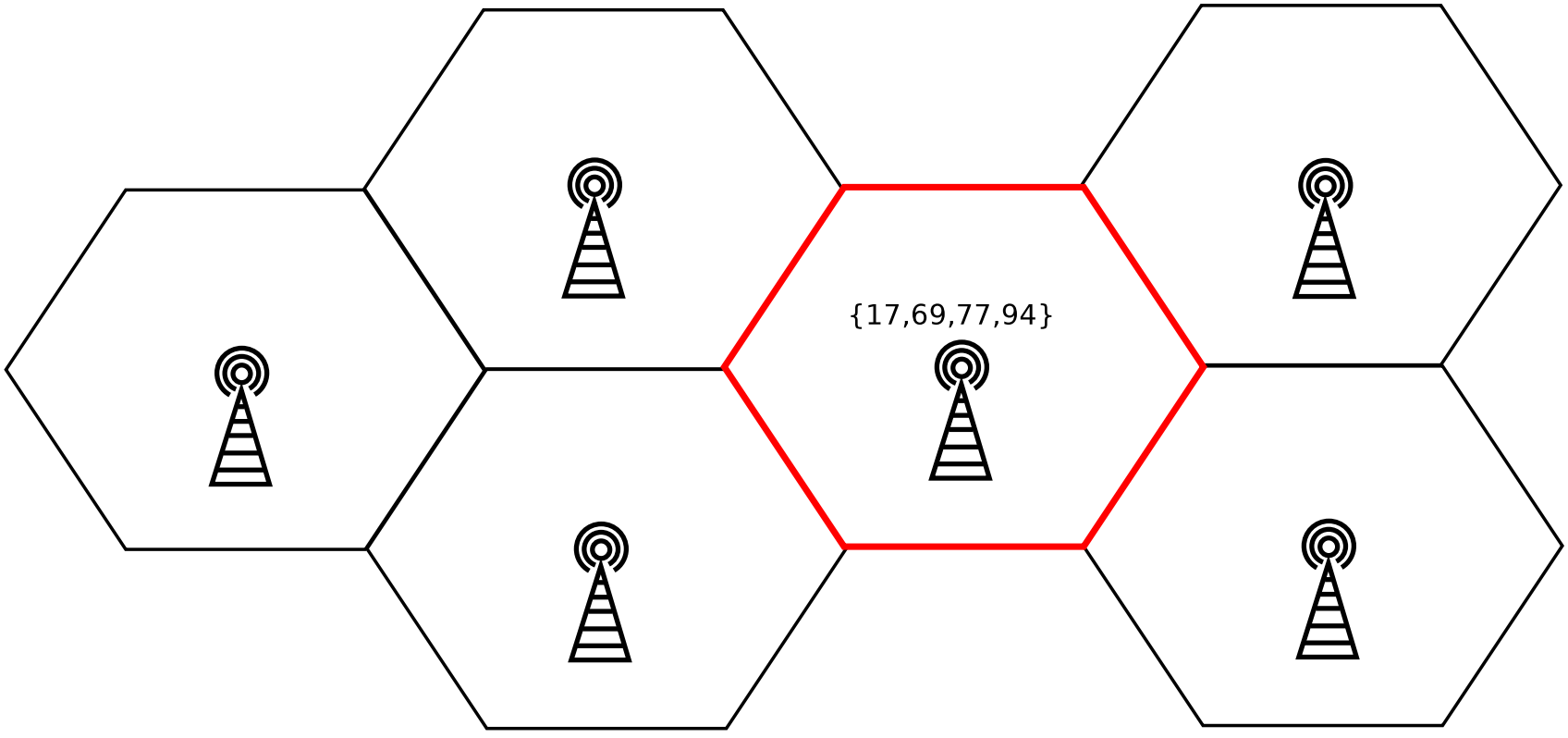
Numbered with ARFCNs



Frequency division



Frequency division



GSM messages

49 06 1b 32 22 02 f4 80 – 11 7f d8 04 28 15 65 04 – a9 00 00 1c 13 2b 2b

55 06 19 00 00 00 00 20 – 00 10 10 00 00 00 00 00 – 01 00 00 a9 00 00 2b

KPN system information

```
1: 49 06 1b 32 22 02 f4 80  – 11 7f d8 04 28 15 65 04 – a9 00 00 1c 13 2b 2b
    0: 49 010010–– Pseudo Length: 18
    1: 06 0––––––– Direction: From originating site
    1: 06 –000–––– 0 TransactionID
    1: 06 ––––0110 Radio Resouce Management
    2: 1b 00011011 RRsystemInfo3C
    3: 32 12834    [0x3222] Cell identity
    5: 02 204      Mobile Country Code (Netherlands)
    6: f4 08f      Mobile Network Code (KPN Telecom B.V.)
    8: 11 4479     [0x117f] Local Area Code
   10: d8 1––––––– Spare bit (should be 0)
   10: d8 –1––––– MSs in the cell shall apply IMSI attach/detach procedure
   10: d8 ––011––– Number of blocks: 3
   10: d8 –––––000 1 basic physical channel for CCCH, not combined with SDCCHs
   11: 04 00000––– spare bits (should be 0)
   11: 04 –––––100 6 multi frames period for paging request
   12: 28 00101000 T3212 TimeOut value: 40
   13: 15 0––––––– spare bit (should be 0)
   13: 15 –0––––– Power control indicator is not set
   13: 15 ––01–––– MSs shall use uplink DTX
   13: 15 ––––0101 Radio Link Timeout: 24
   14: 65 011––––– Cell Reselect Hyst. :  6 db RXLEV
   14: 65 –––xxxxx Max Tx power level: 5
   15: 04 0––––––– No additional cells in SysInfo 7–8
   15: 04 –0––––– New establishm cause: not supported
   15: 04 ––xxxxxx RXLEV Access Min permitted = –110 + 4dB
   16: a9 10––––– Max. of retransmiss : 4
   16: a9 ––1010–– slots to spread TX : 14
   16: a9 ––––––0– The cell is barred  : no
   16: a9 –––––––1 Cell reestabl.i.cell: not allowed
   17: 00 –––––0–– Emergency call EC 10: allowed
   17: 00 00000––– Acc ctrl cl 11–15: 0 = permitted, 1 = forbidden
   17: 00 ––––––00 Acc ctrl cl  8– 9: 0 = permitted, 1 = forbidden
   17: 00 –––––––0 Ordinary subscribers (8)
```

KPN system information

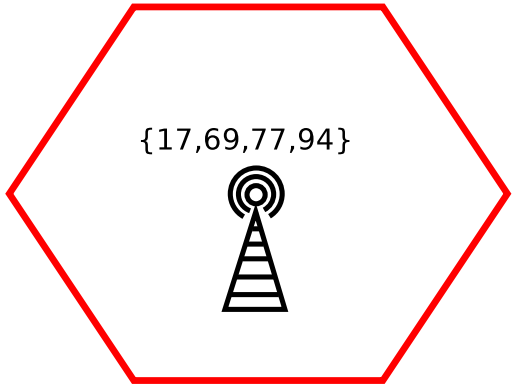
```
2: 55 06 19 00 00 00 00 20  – 00 10 10 00 00 00 00 00 – 01 00 00 a9 00 00 2b
    0: 55 010101–– Pseudo Length: 21
    1: 06 0––––––– Direction: From originating site
    1: 06 –000–––– 0 TransactionID
    1: 06 ––––0110 Radio Resouce Management
    2: 19 00011001 RRsystemInfo1
    3: 00 00––––––– Bitmap 0 format
    7: 20 ––1––––– Cell Allocation      : ARFCN 94
    9: 10 ––––1–––– Cell Allocation      : ARFCN 77
   10: 10 ––––1–––– Cell Allocation      : ARFCN 69
   16: 01 –––––––1 Cell Allocation      : ARFCN 17
   19: a9 10––––––– Max. of retransmiss : 4
   19: a9 ––1010–– slots to spread TX : 14
   19: a9 ––––––0– The cell is barred  : no
   19: a9 –––––––1 Cell reestabl.i.cell: not allowed
   20: 00 –––––0–– Emergency call EC 10: allowed
   20: 00 00000––– Acc ctrl cl 11–15: 0 = permitted, 1 = forbidden
   20: 00 ––––––00 Acc ctrl cl  8– 9: 0 = permitted, 1 = forbidden
   20: 00 –––––––0 Ordinary subscribers (8)
   20: 00 ––––––0– Ordinary subscribers (9)
   20: 00 –––––0–– Emergency call (10): Everyone
   20: 00 ––––0––– Operator Specific (11)
   20: 00 –––0–––– Security service (12)
   20: 00 ––0––––– Public service (13)
   20: 00 –0––––––  Emergency service (14)
   20: 00 0––––––– Network Operator (15)
   21: 00 00000000 Acc ctrl cl  0– 7: 0 = permitted, 1 = forbidden
   21: 00 00000000 Ordinary subscribers (0–7)
```

KPN system information

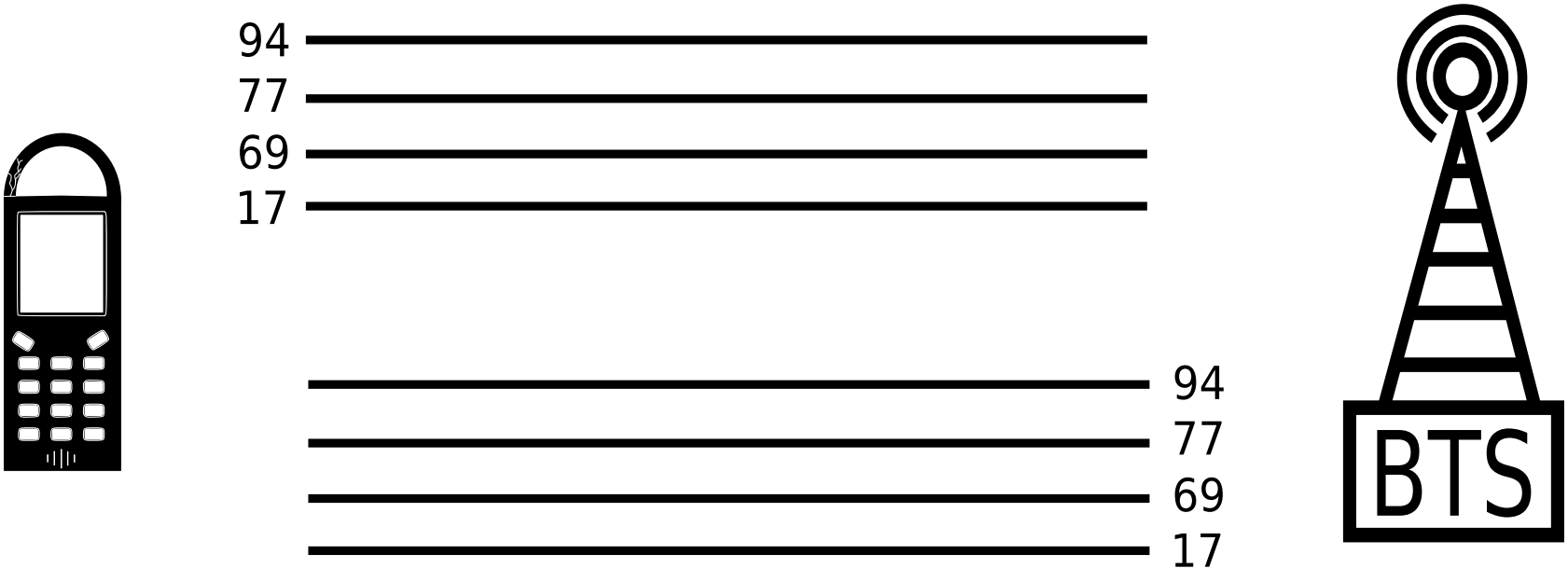
```
[0x3222] Cell identity
 Mobile Country Code (Netherlands)
 Mobile Network Code (KPN Telecom B.V.)
[0x117f] Local Area Code


Cell Allocation      : ARFCN 94
Cell Allocation      : ARFCN 77
Cell Allocation      : ARFCN 69
Cell Allocation      : ARFCN 17
```

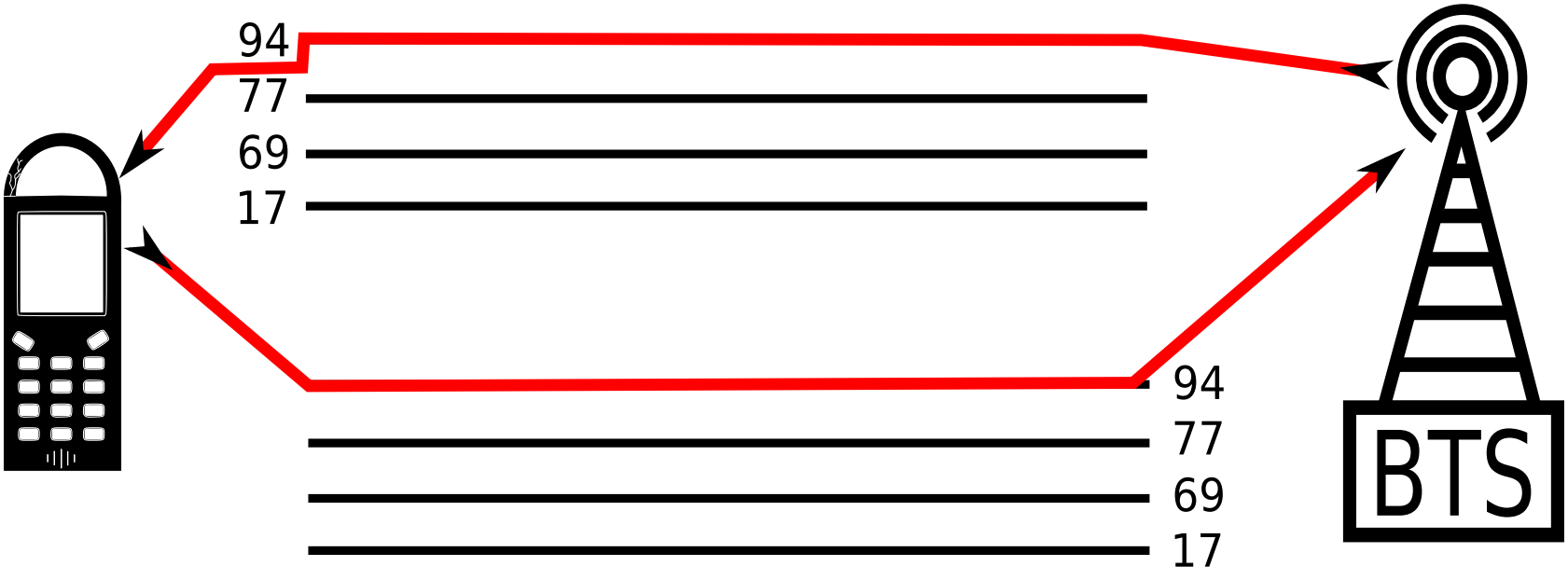
The KPN cell



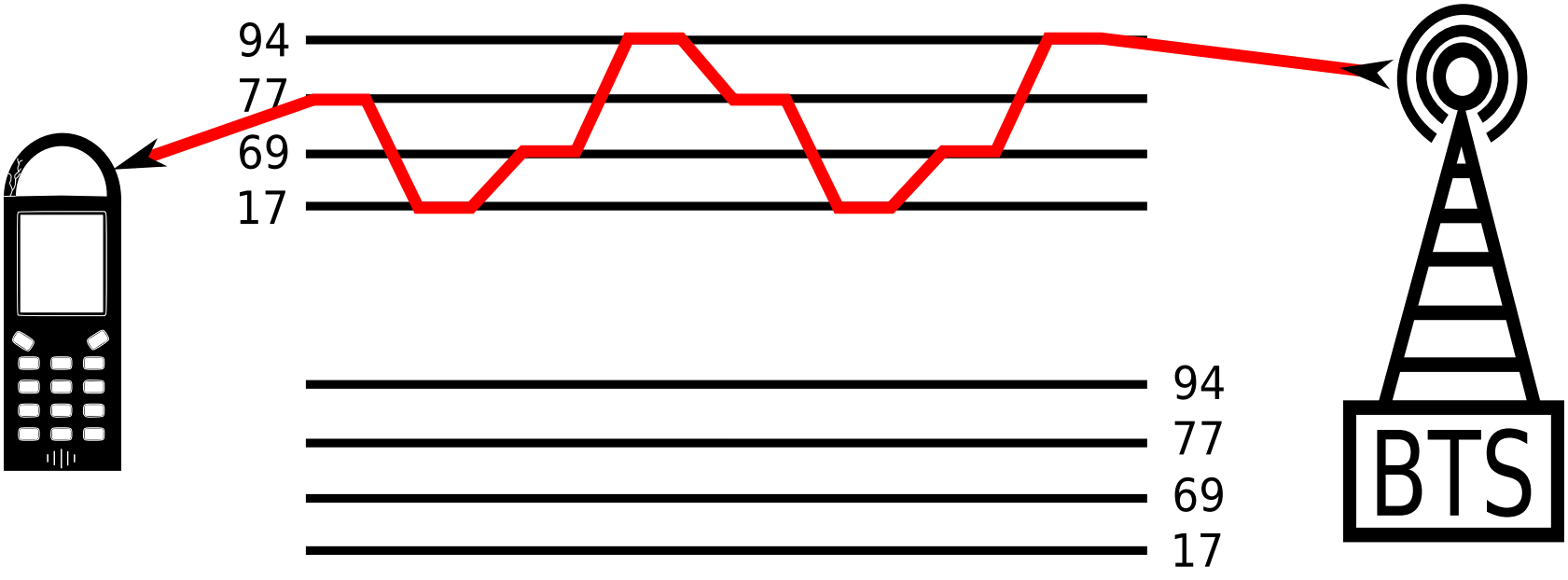
The KPN cell



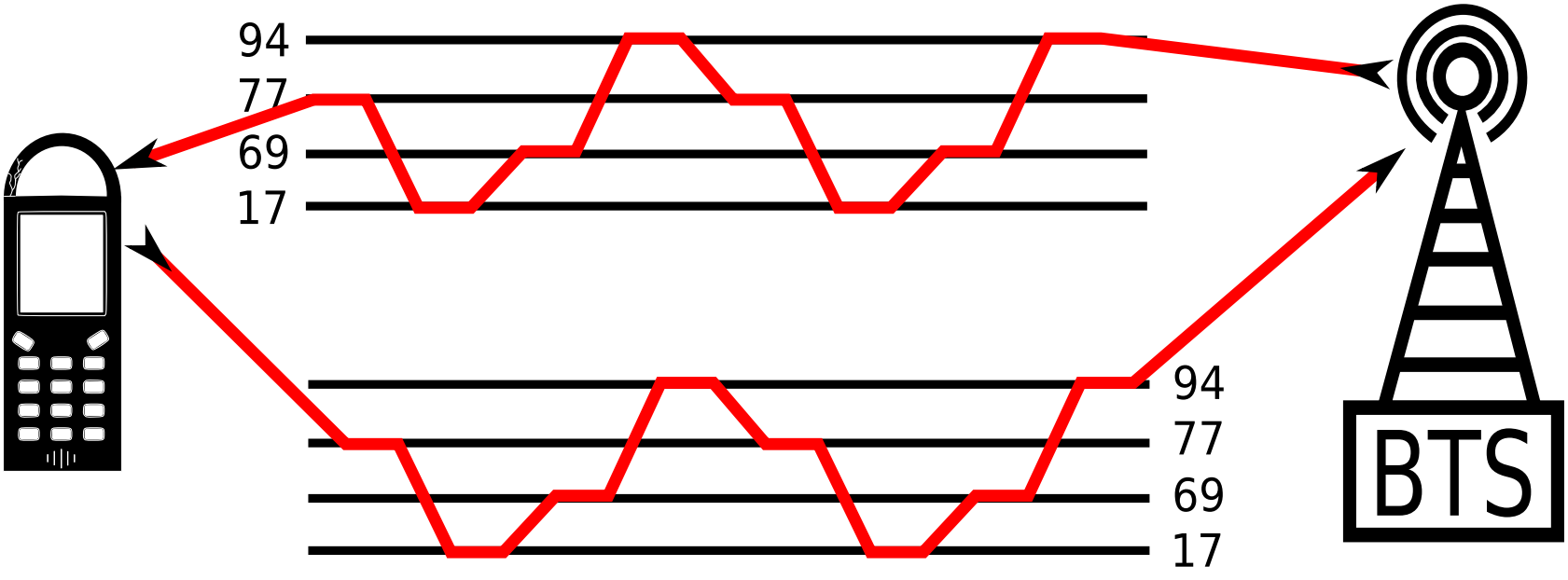
No Frequency hopping



Frequency hopping (I)



Frequency hopping (II)



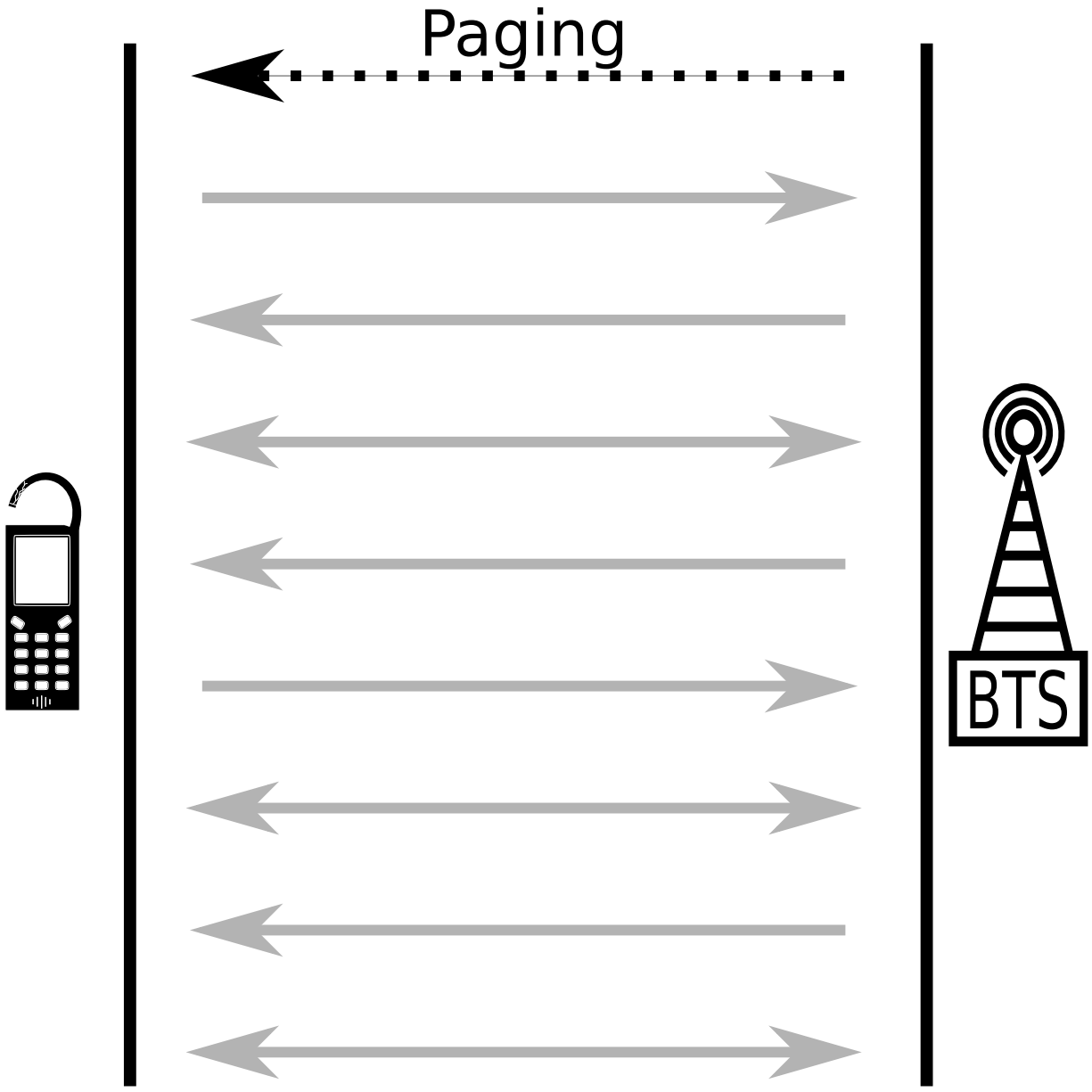
Immediate Assignment

```
31 06 3f 00 52 f0 ab 85  - ad e0 01 01 0f 2b 2b 2b - 2b 2b 2b 2b 2b 2b 2b
    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: 3f 0-111111 RRimmediateAssignment
    2: 3f -x------ Send sequence number: 0
    3: 00 ------00 Page Mode: Normal paging
    3: 00 -0------ No meaning
    3: 00 --0----- Downlink assign to MS: No meaning
    3: 00 ---0---- This messages assigns a dedicated mode resource
    4: 52 -----010 Timeslot number: 2
    4: 52 01010--- Chan. Descript.: SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8)
    5: f0 111----- Training seq. code : 7
    5: f0 ---1---- HoppingChannel
    6: ab ........ Mobile Allocation Index Offset (MAIO) 2
    6: ab --101011 Hopping Seq. Number: 43
    7: 85 100----- Establishing Cause: Answer to paging
    7: 85 ---xxxxx Random Reference : 5
    8: ad xxxxxxxx T1/T2/T3
    9: e0 xxxxxxxx T1/T2/T3
   10: 01 --xxxxxx Timing advance value: 1
   11: 01 00000001 Length of Mobile Allocation: 1
   12: 0f ----1--- Mobile Allocation ARFCN #4
   12: 0f -----1-- Mobile Allocation ARFCN #3
   12: 0f ------1- Mobile Allocation ARFCN #2
   12: 0f -------1 Mobile Allocation ARFCN #1
```

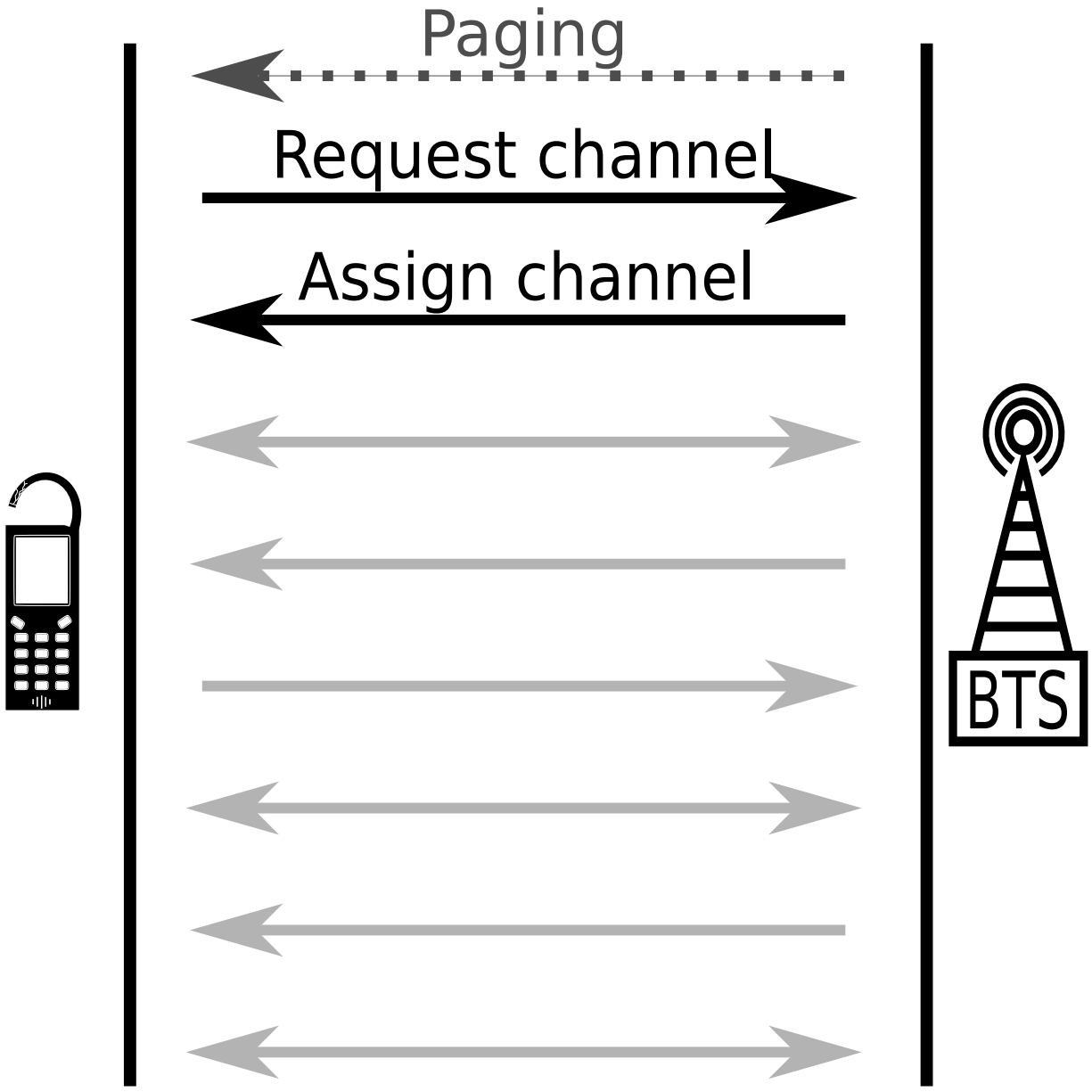
Immediate Assignment

```
HoppingChannel
Mobile Allocation Index Offset (MAIO) 2
Hopping Seq. Number: 43
Mobile Allocation ARFCN #4
Mobile Allocation ARFCN #3
Mobile Allocation ARFCN #2
Mobile Allocation ARFCN #1
```

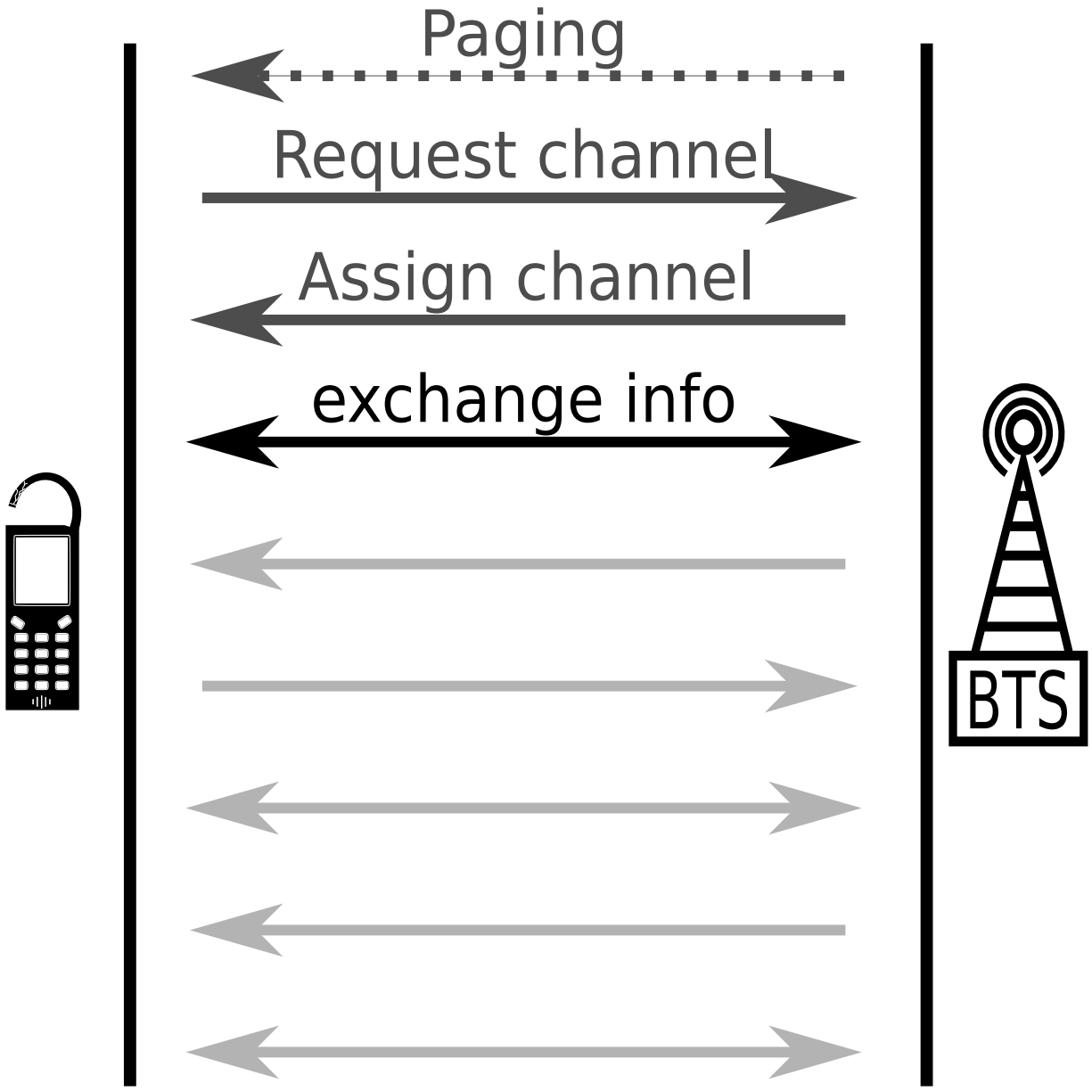
Message Sequence



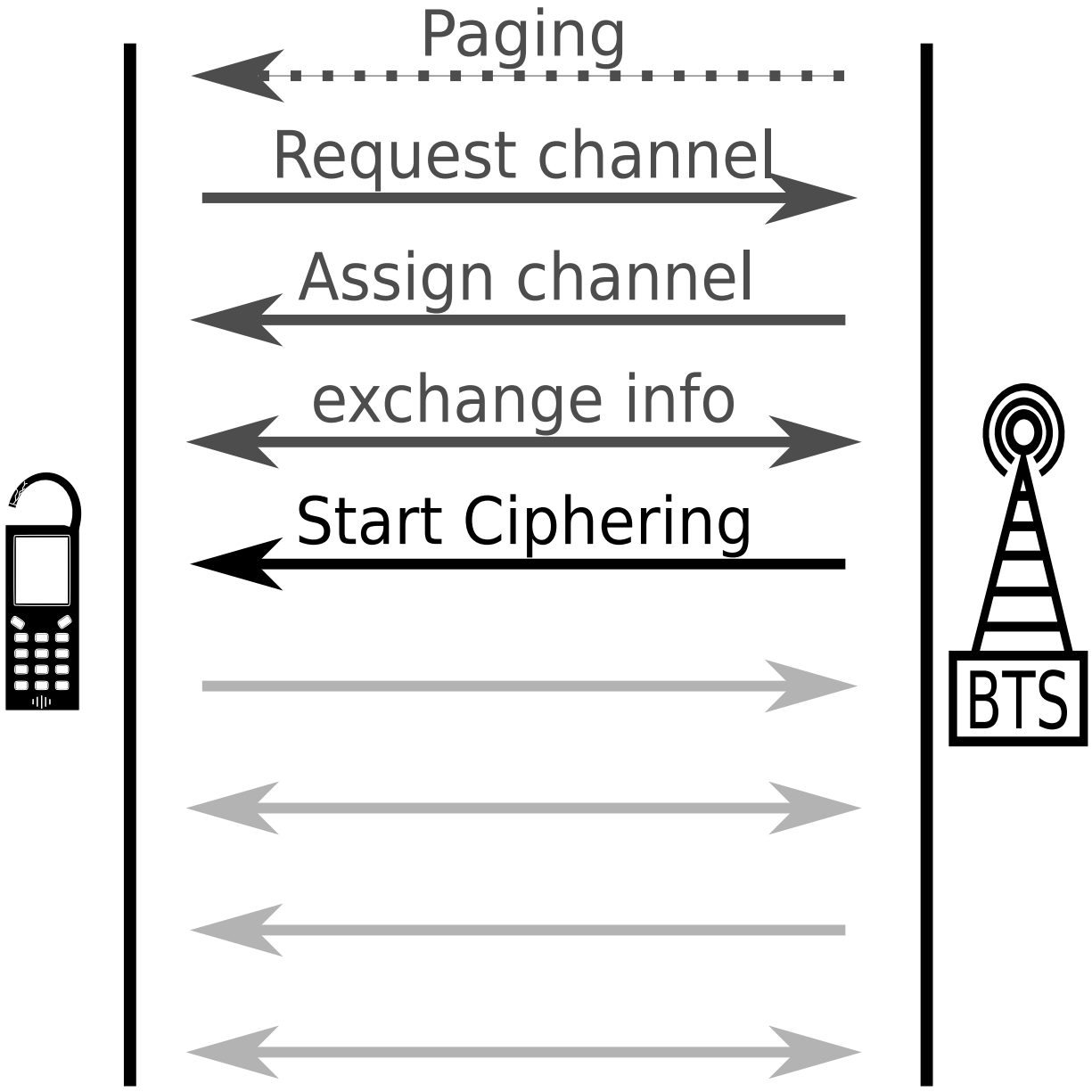
Message Sequence



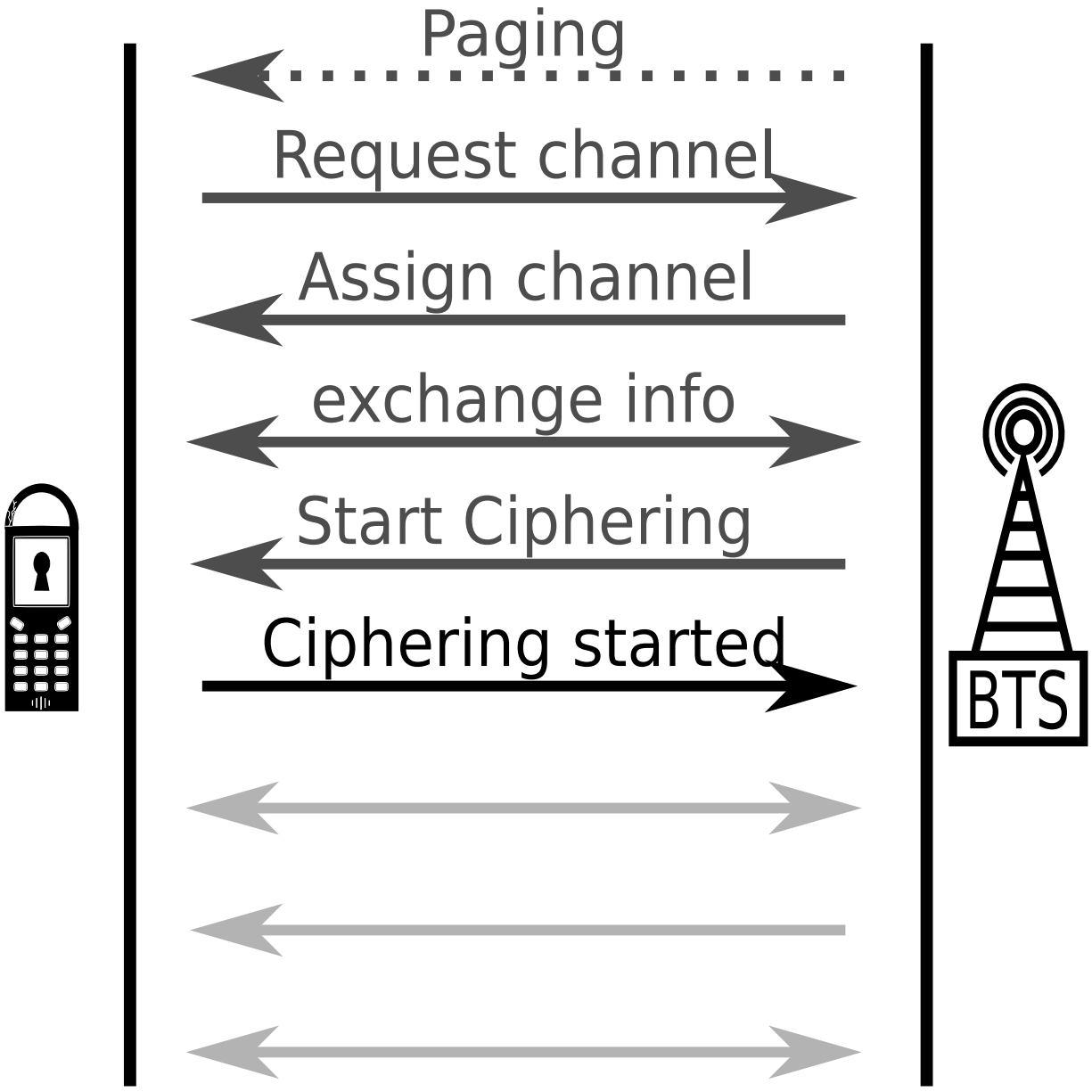
Message Sequence



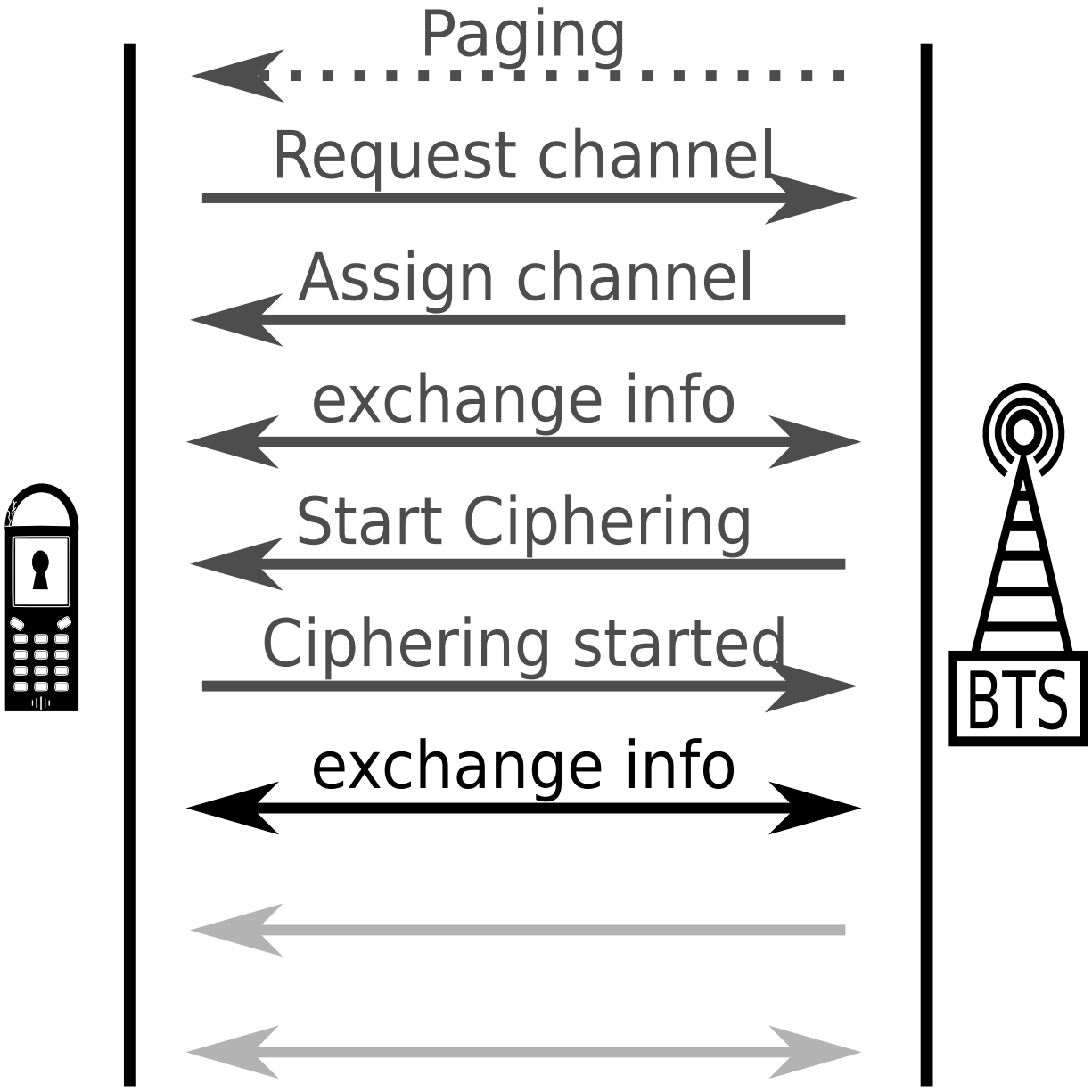
Message Sequence



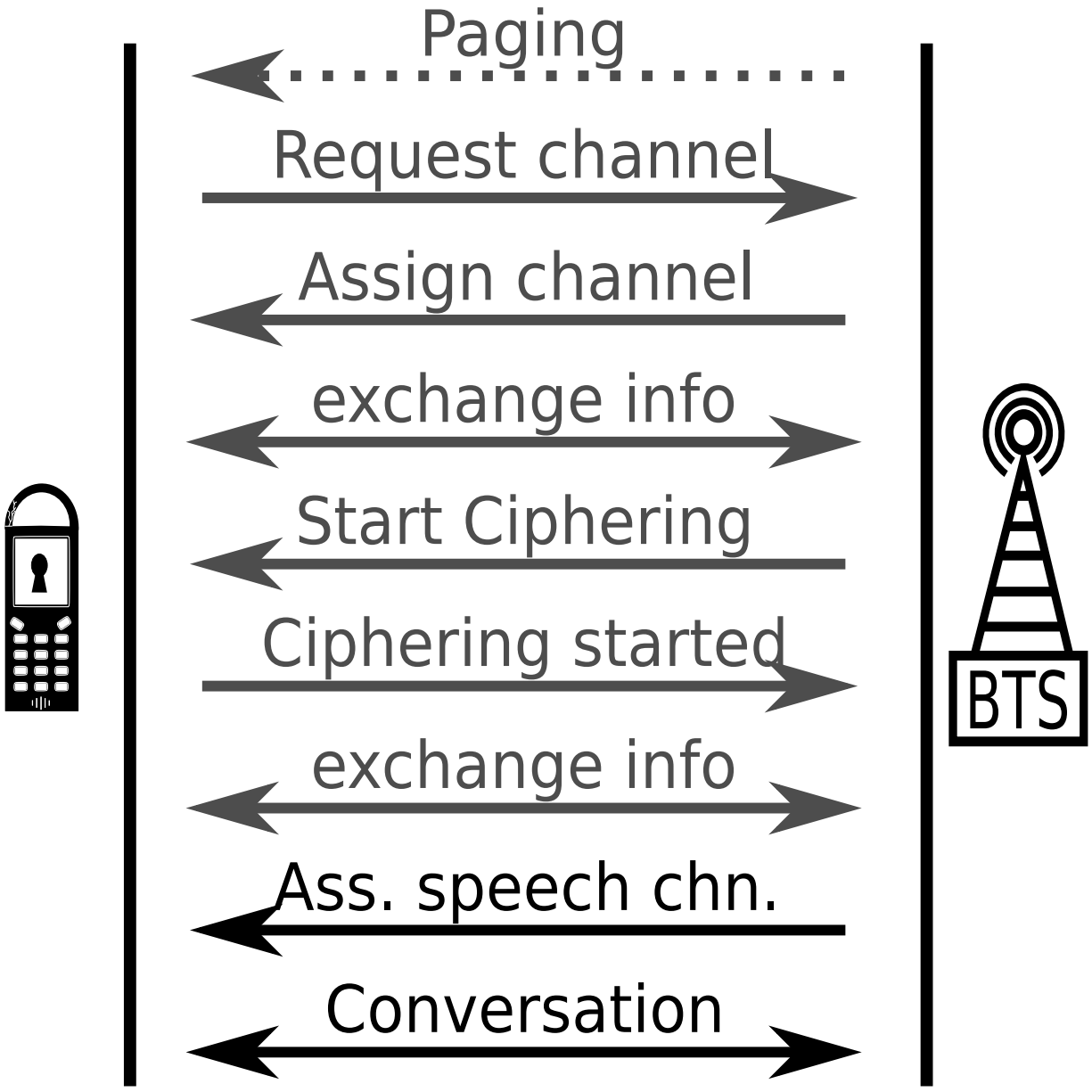
Message Sequence



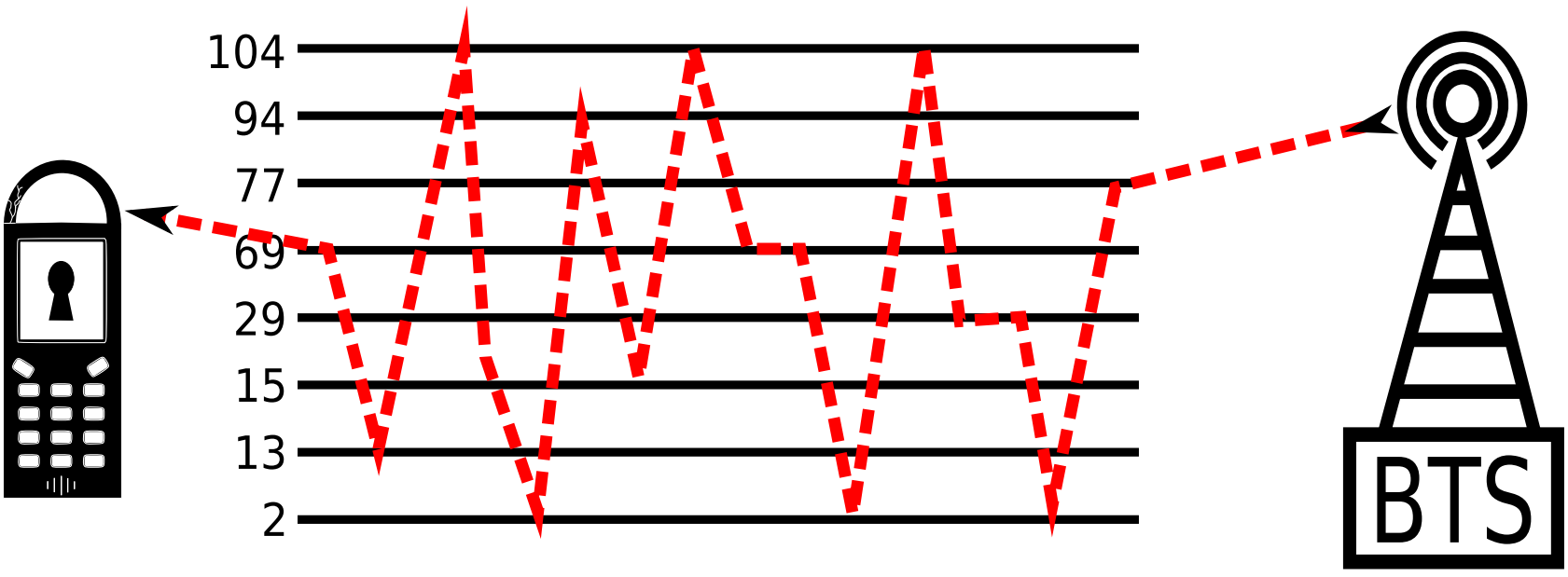
Message Sequence



Message Sequence



Hopping Problem

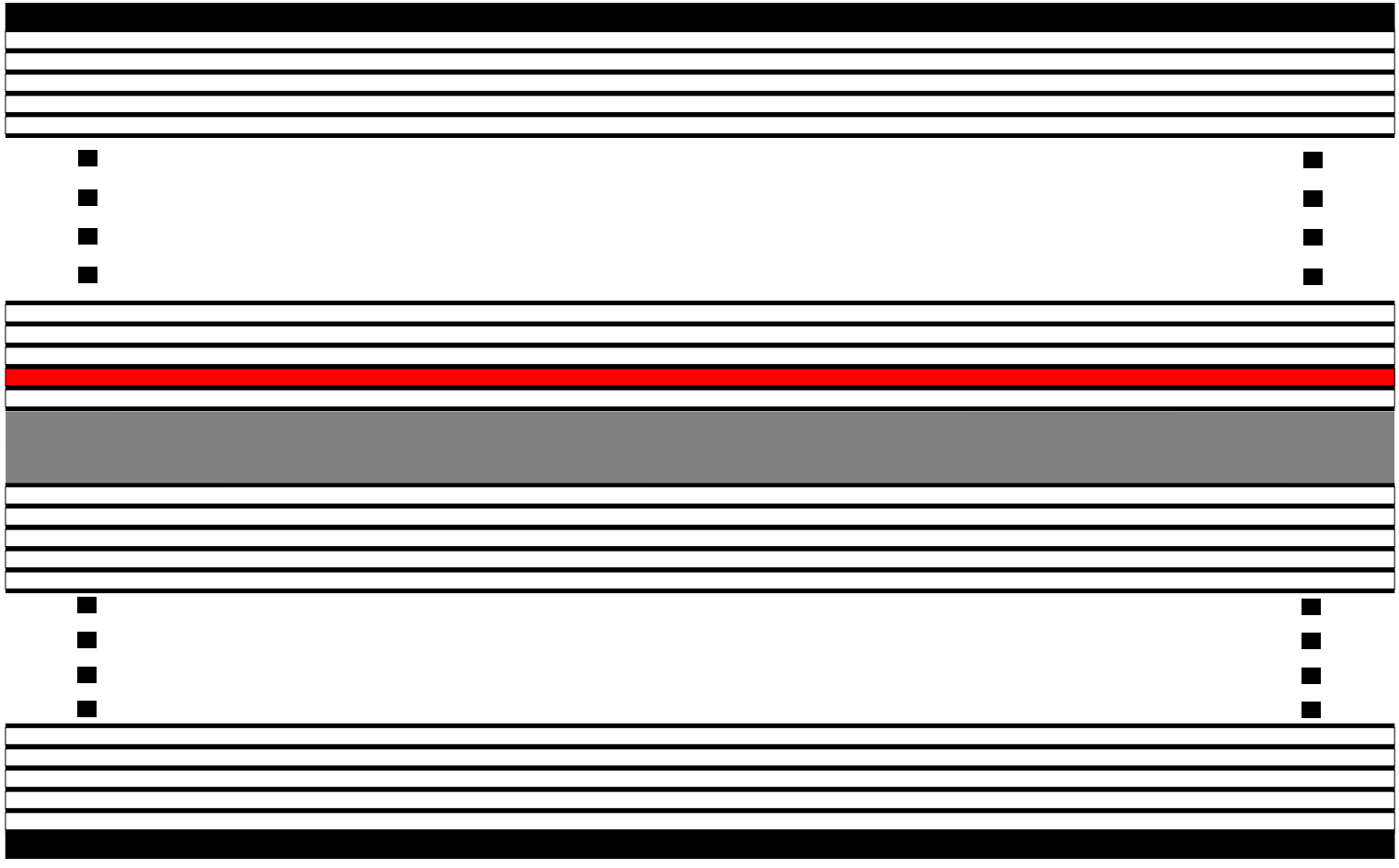


Conclusion

- Still hard to eavesdrop in general
- Other attacks have become feasible
- The GSM system can still use a lot of testing

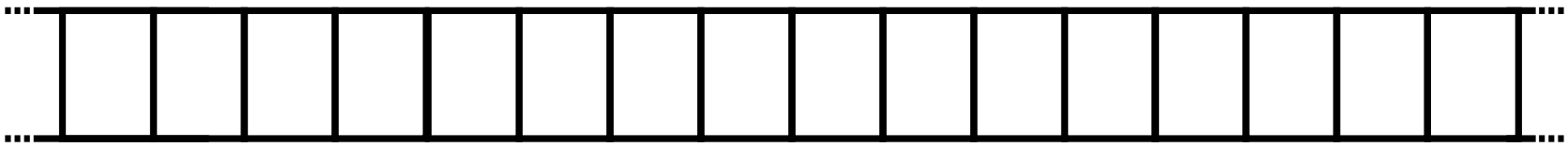
Questions

A single sub-frequency

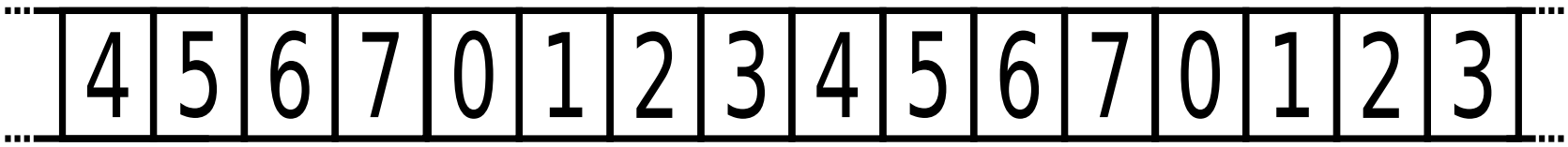


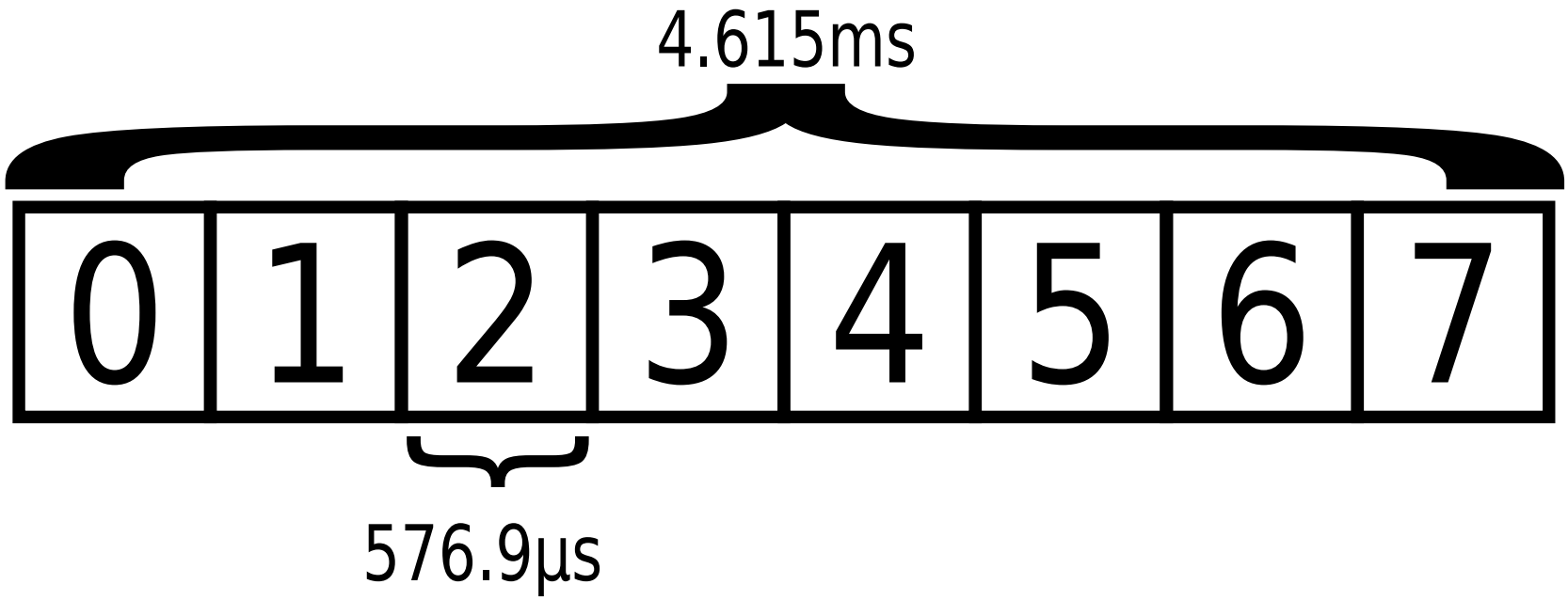
A single sub-frequency

Time division

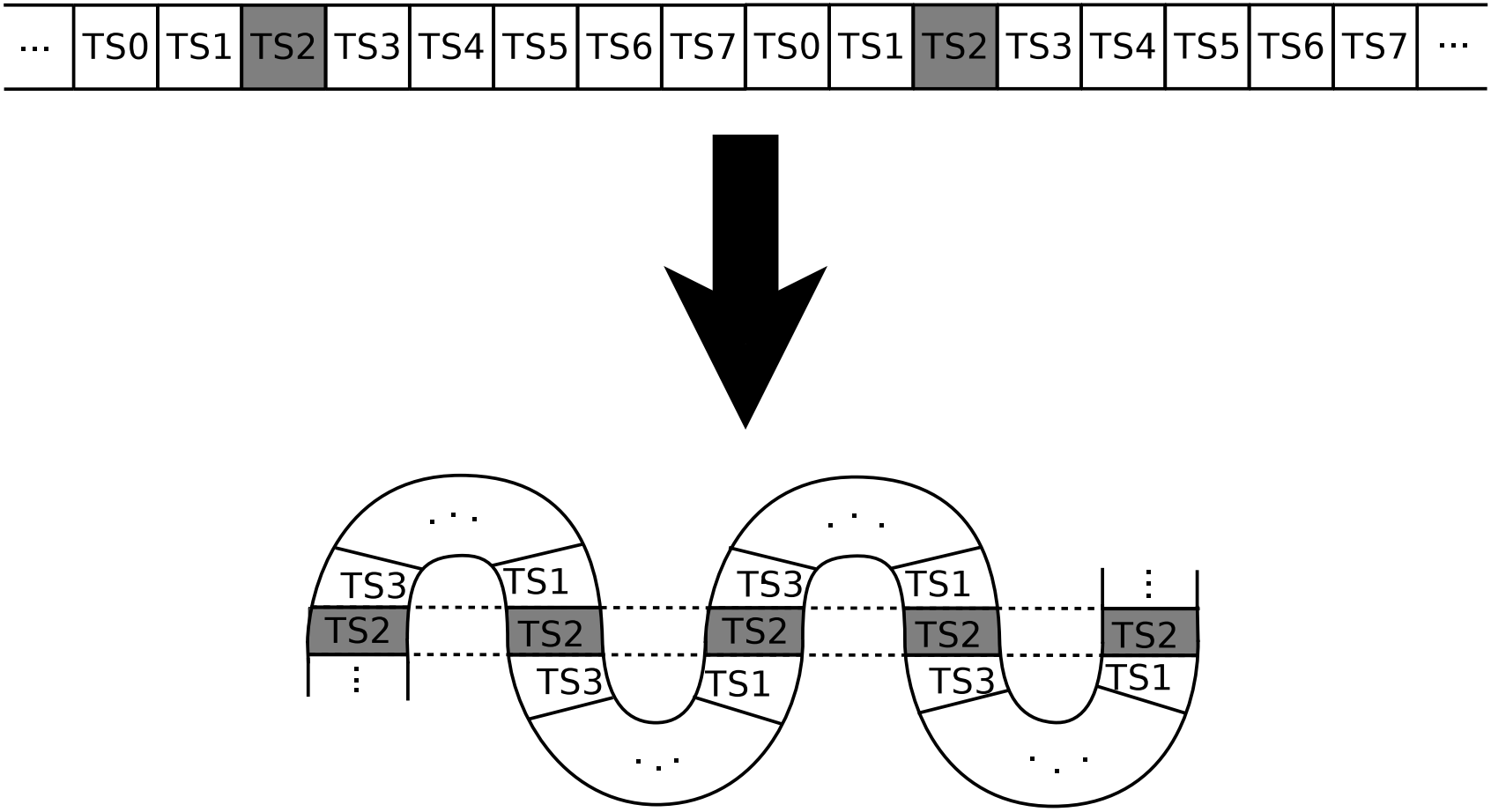


Time division




4.615ms
0
1
2
3
4
5
6
7
576.9µs

Logical channels



Offset