GSM SECURITY: FACT AND FICTION

BruCON 2010

Fabian van den Broek

Radboud University Nijmegen
Institute for Computing and Information Sciences (iCIS)

24 September 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

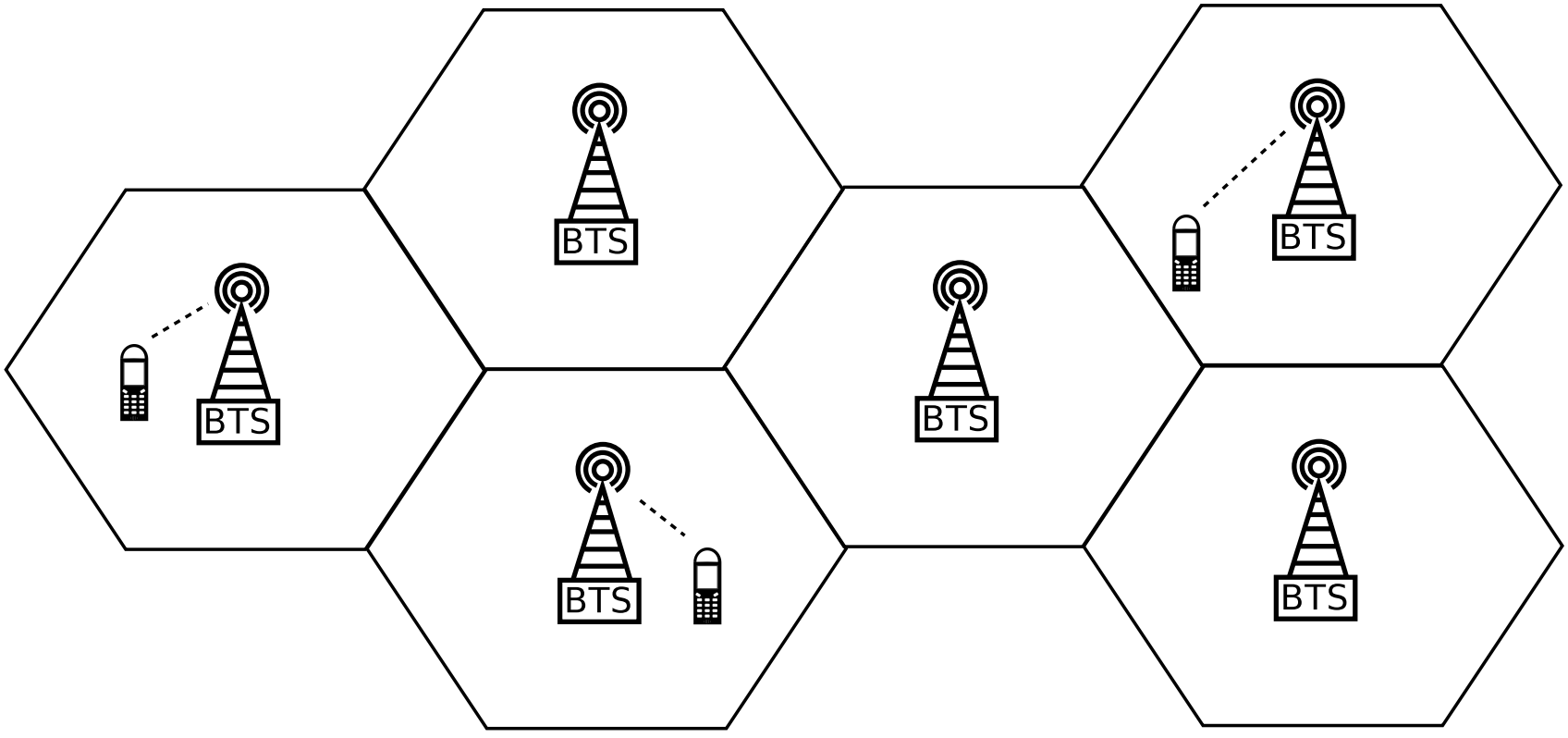
But has GSM been properly tested?

Outline of this talk

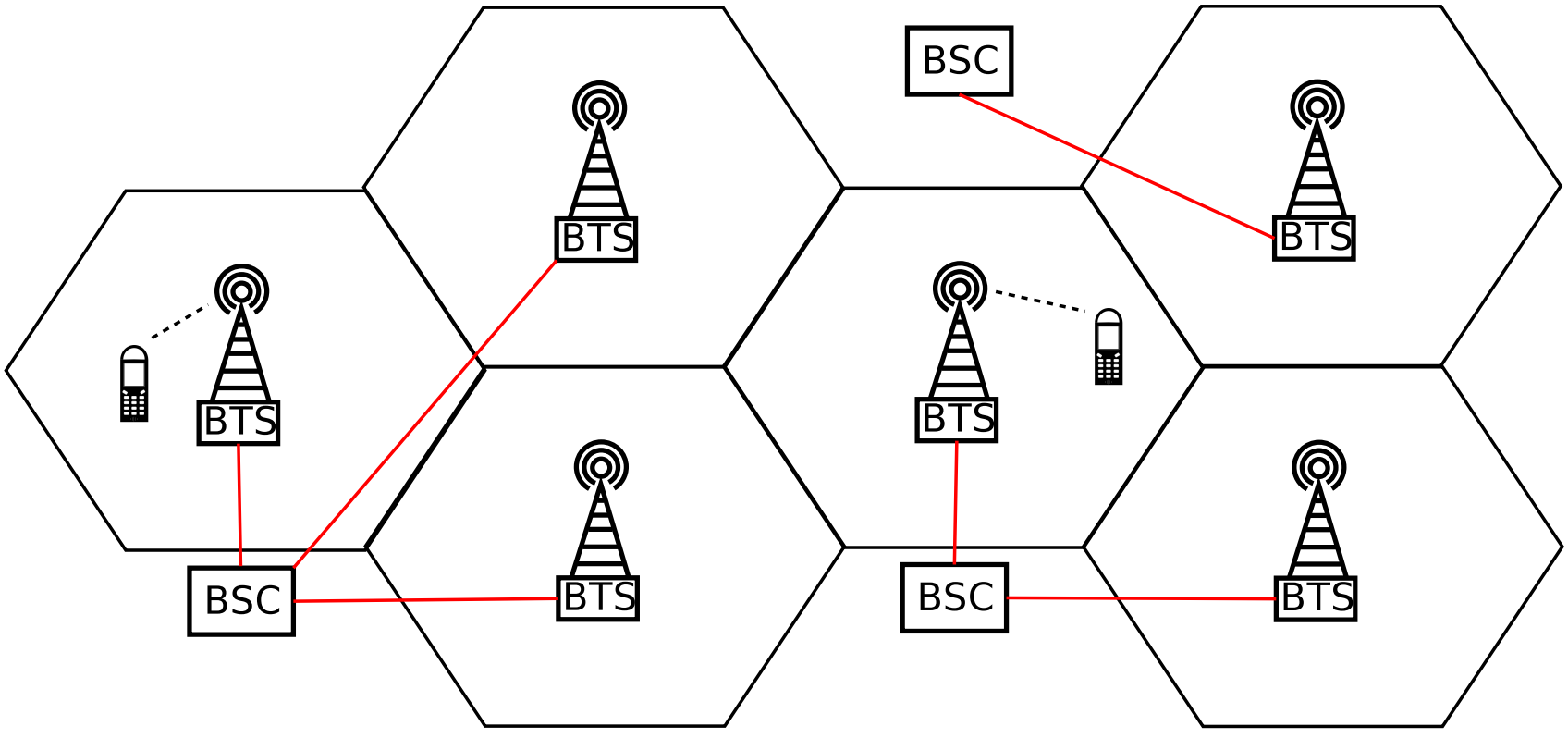
- GSM overview
- GSM security
- Attacks
- Conclusion

GSM overview

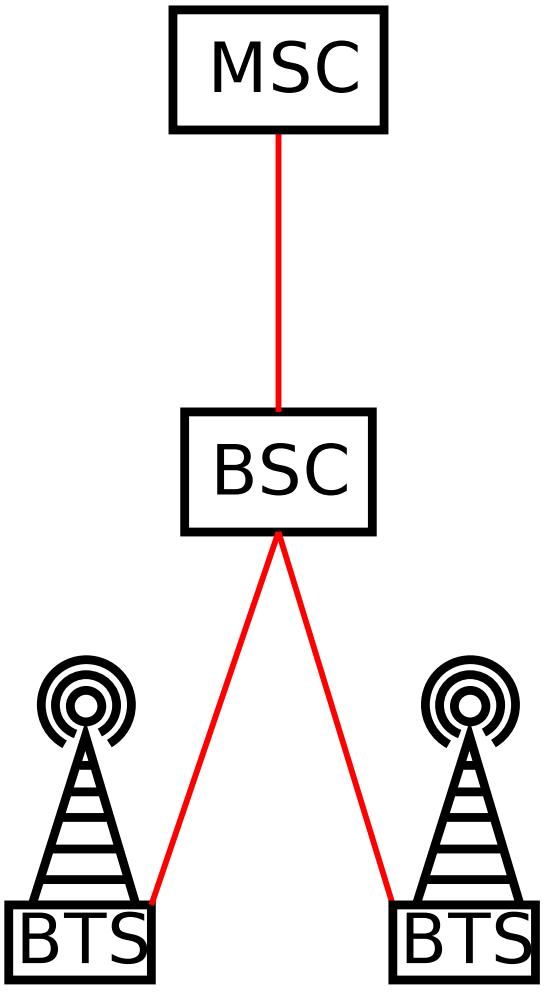
Cellular technology

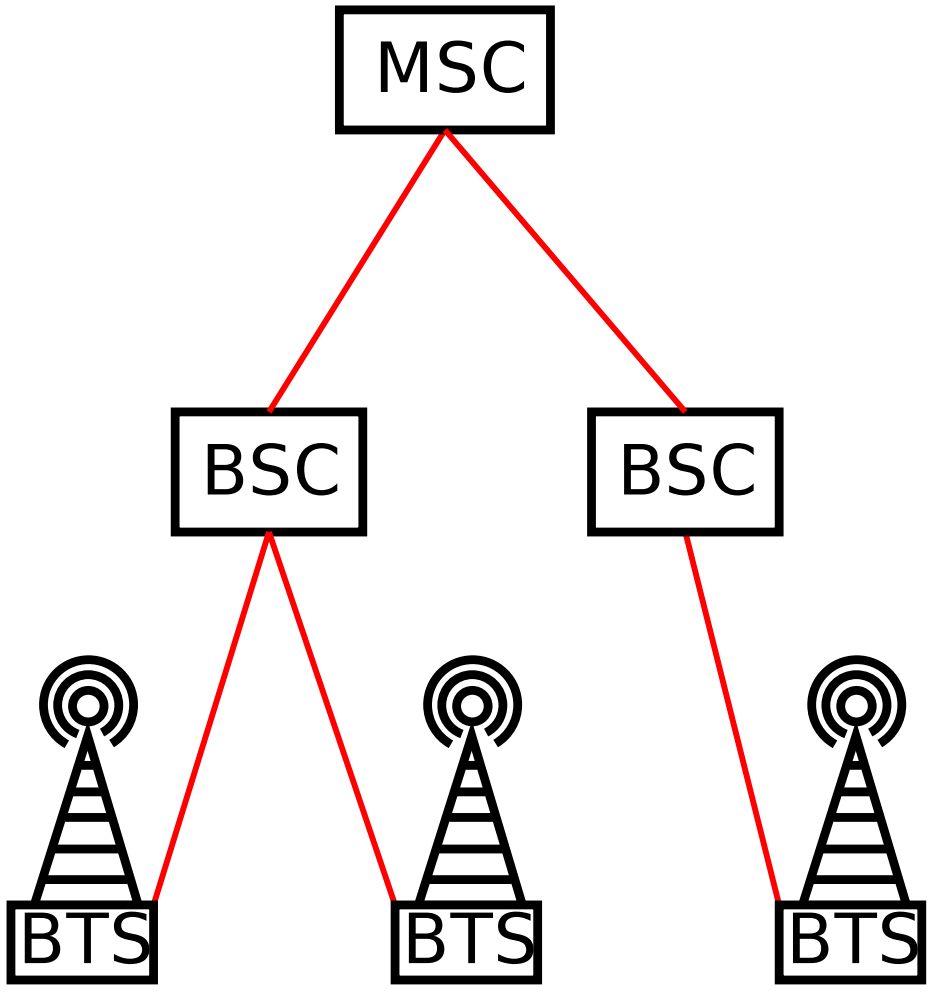


Cellular technology

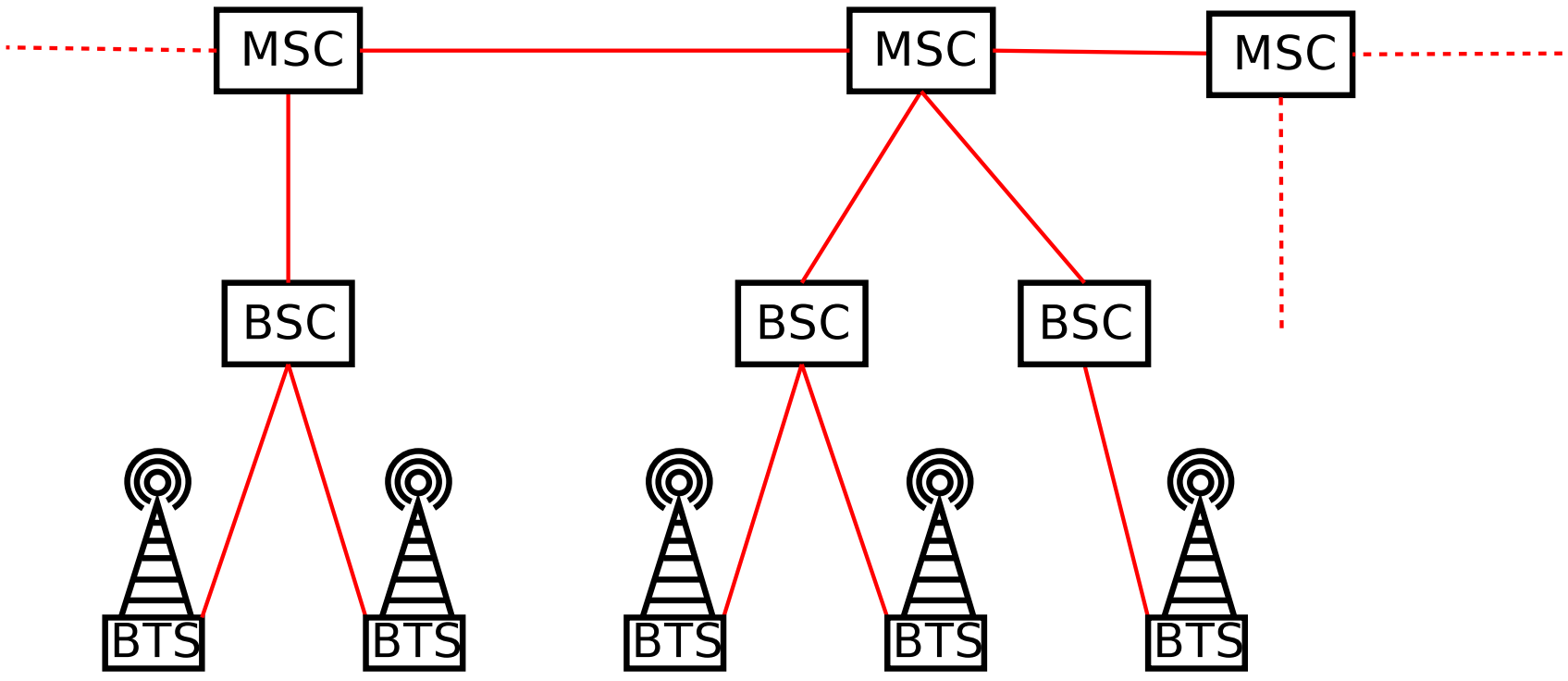


Cellular technology

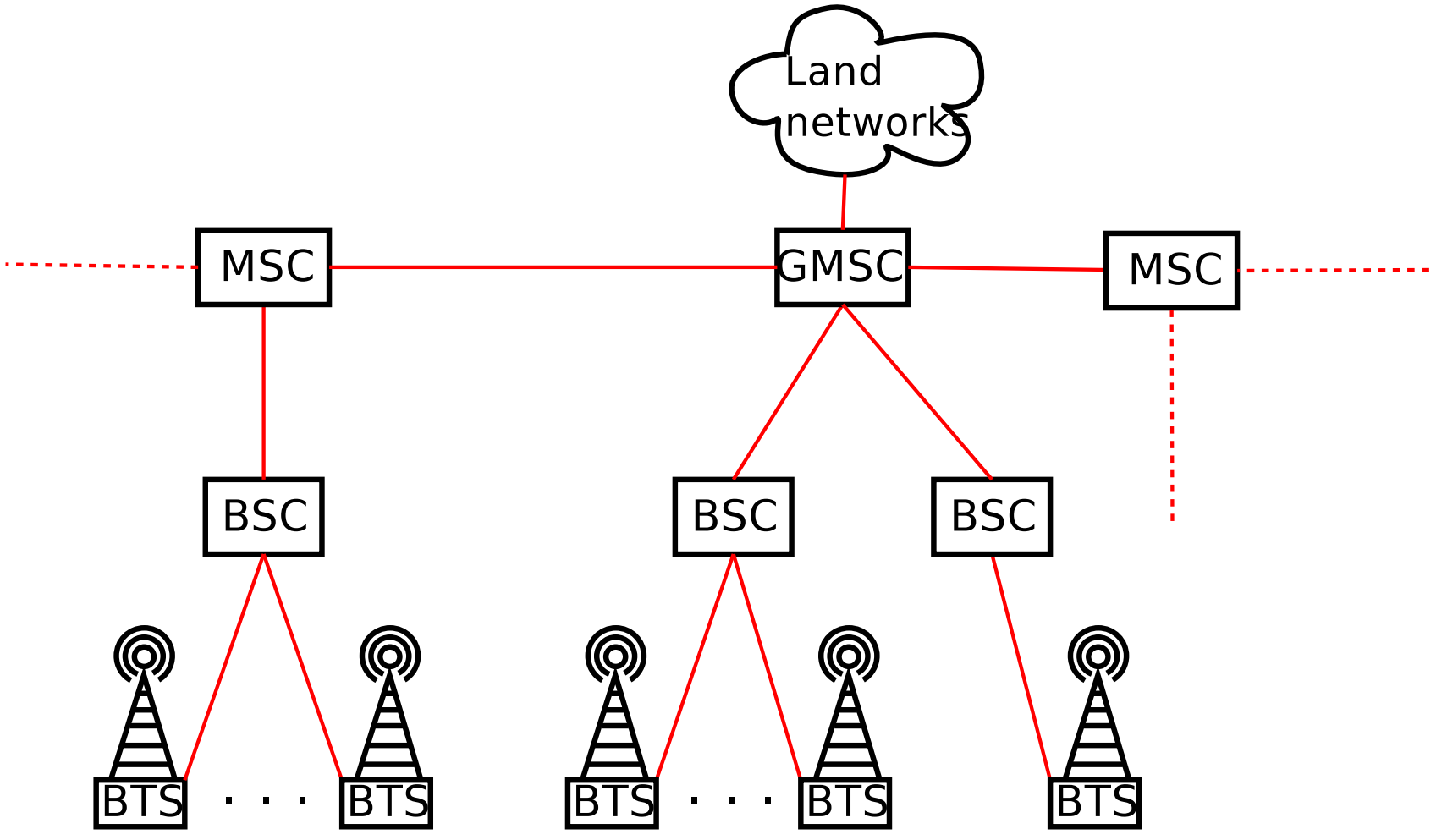




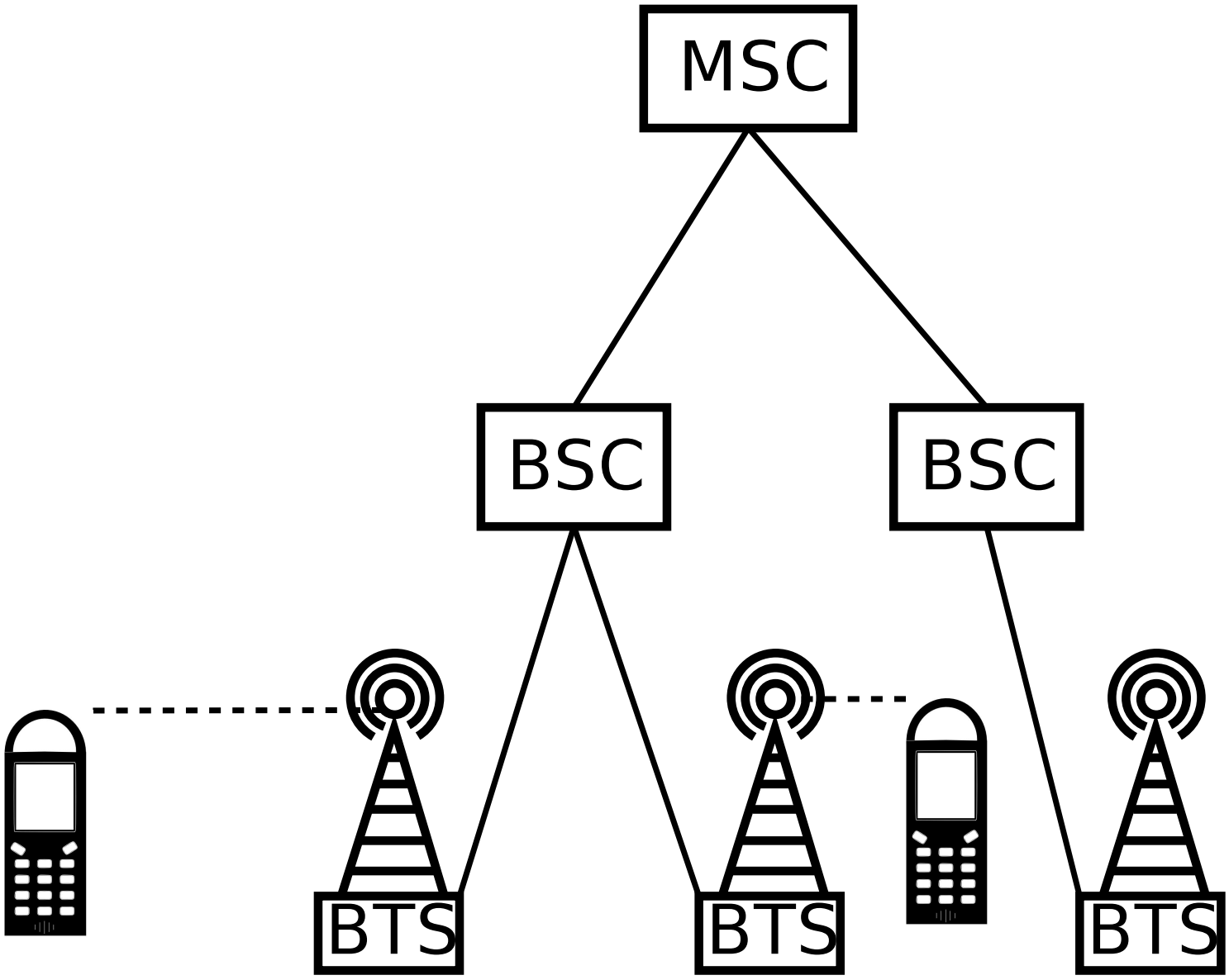
Cellular technology



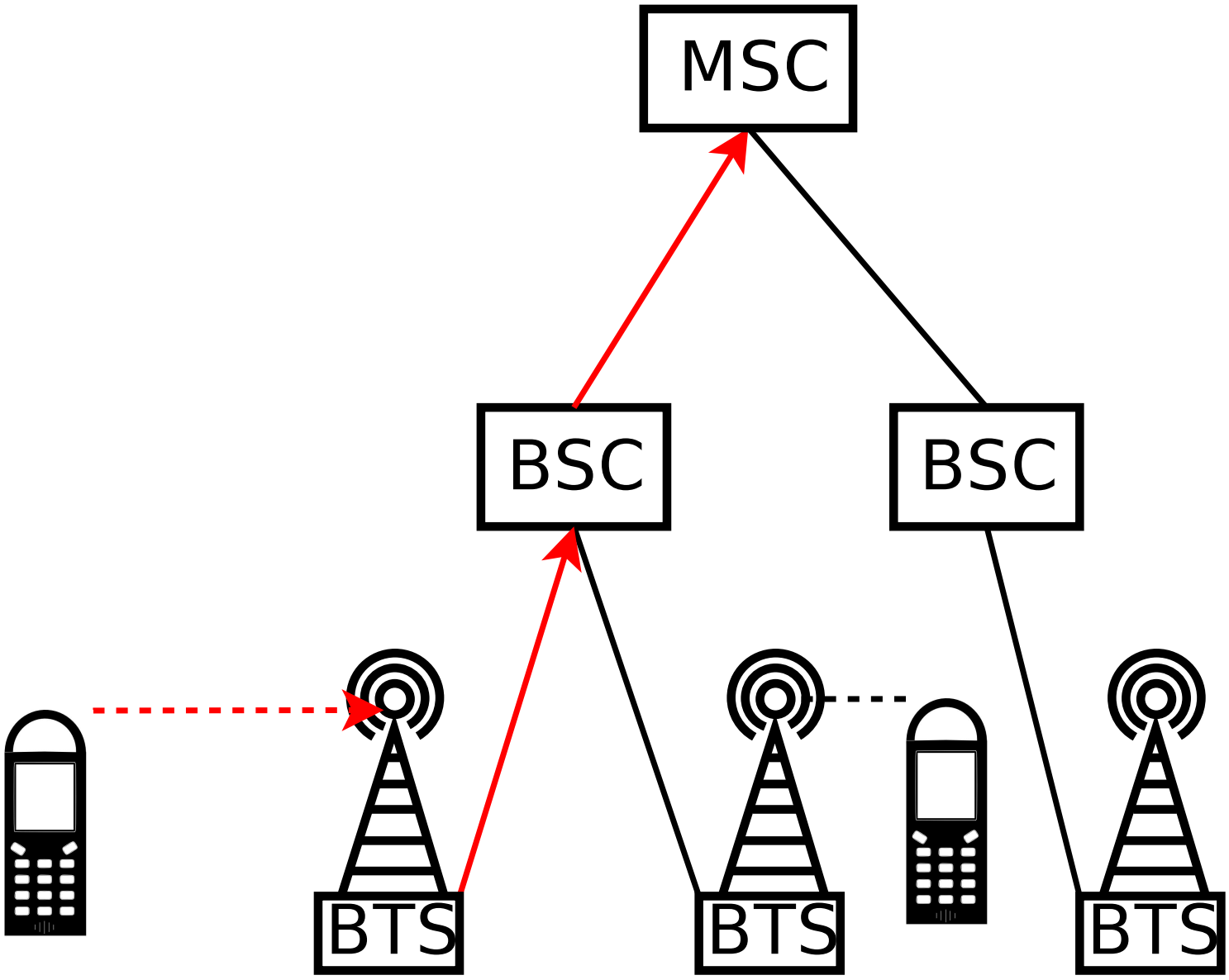
Cellular technology



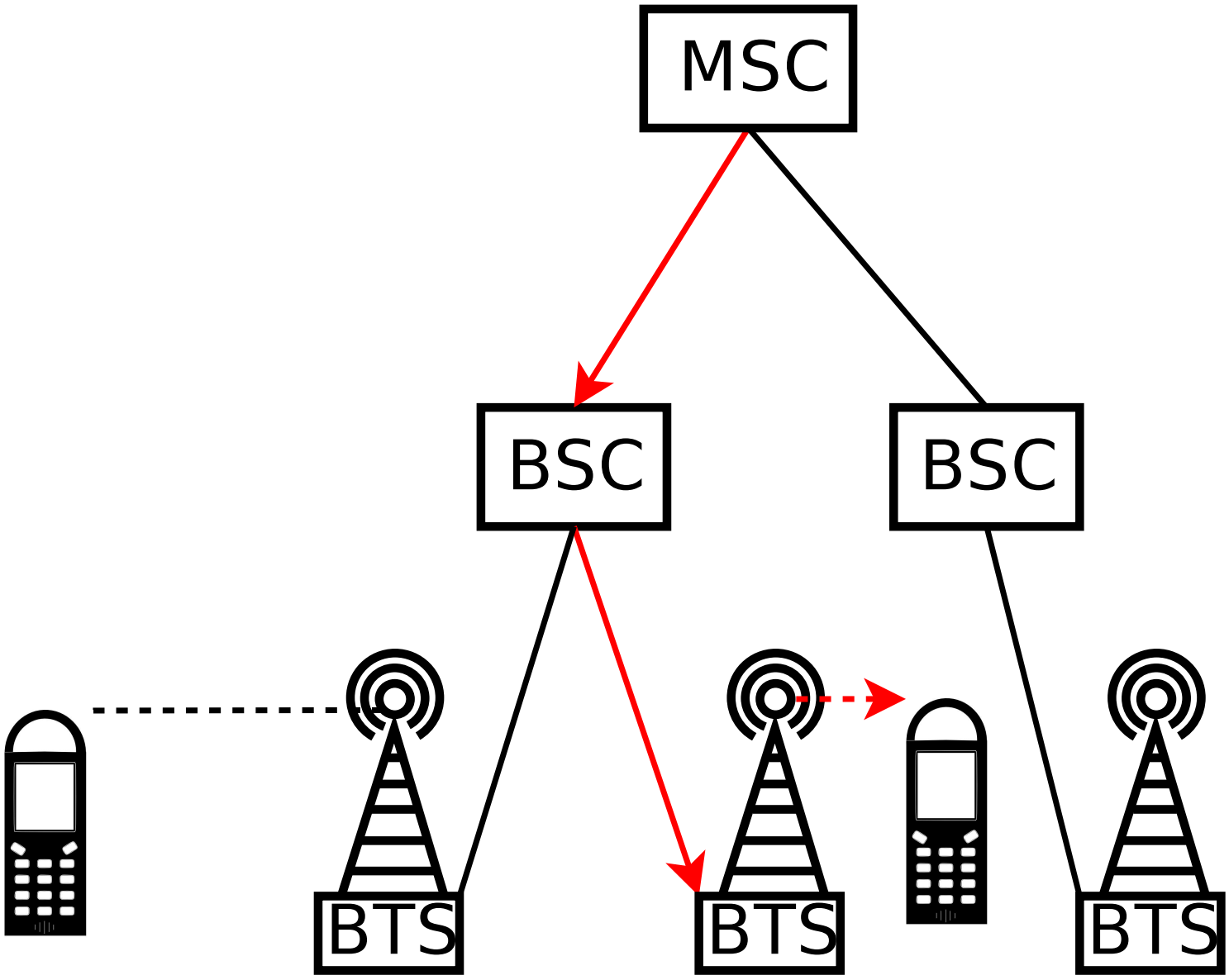
Phone call routing



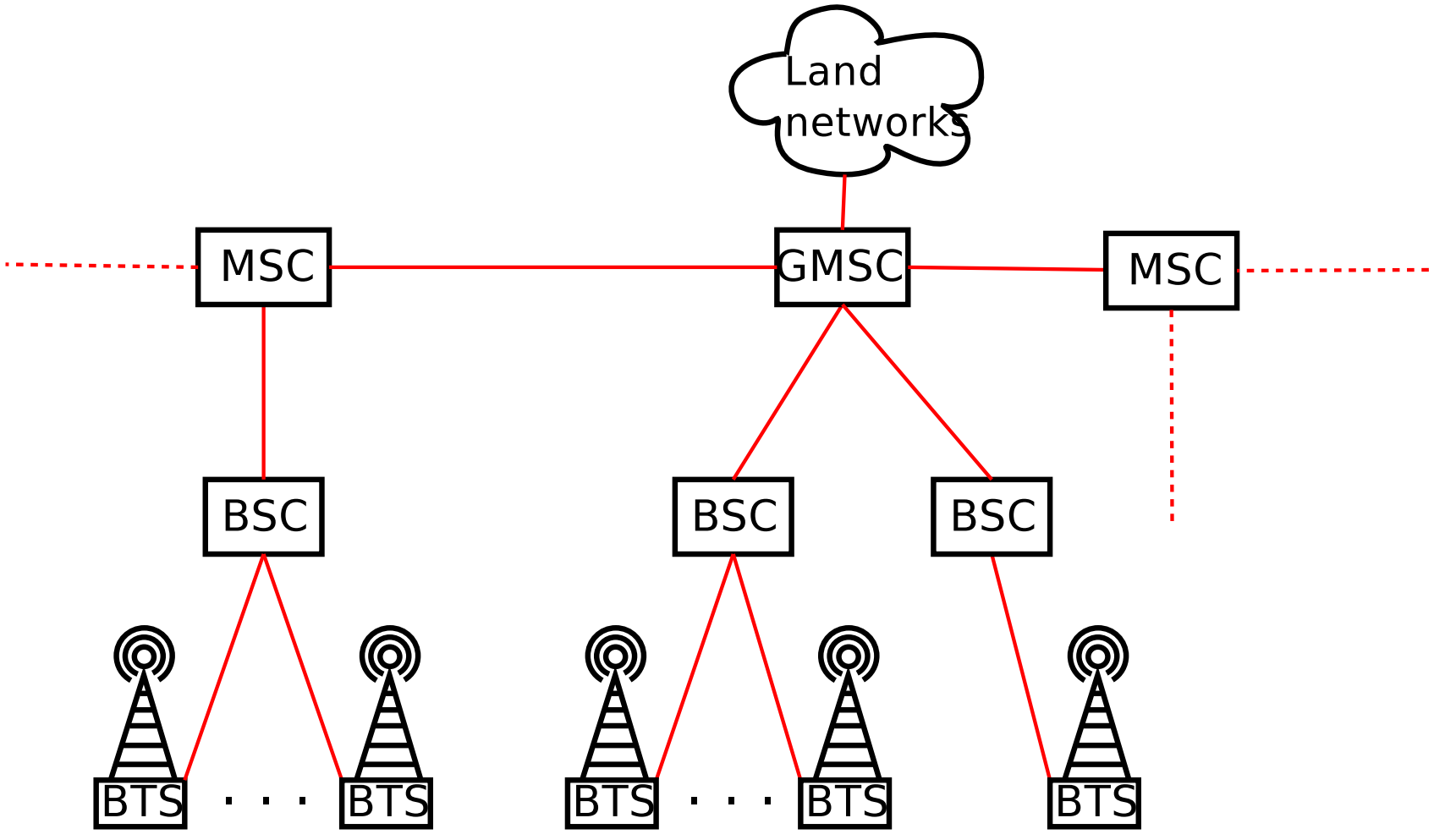
Phone call routing



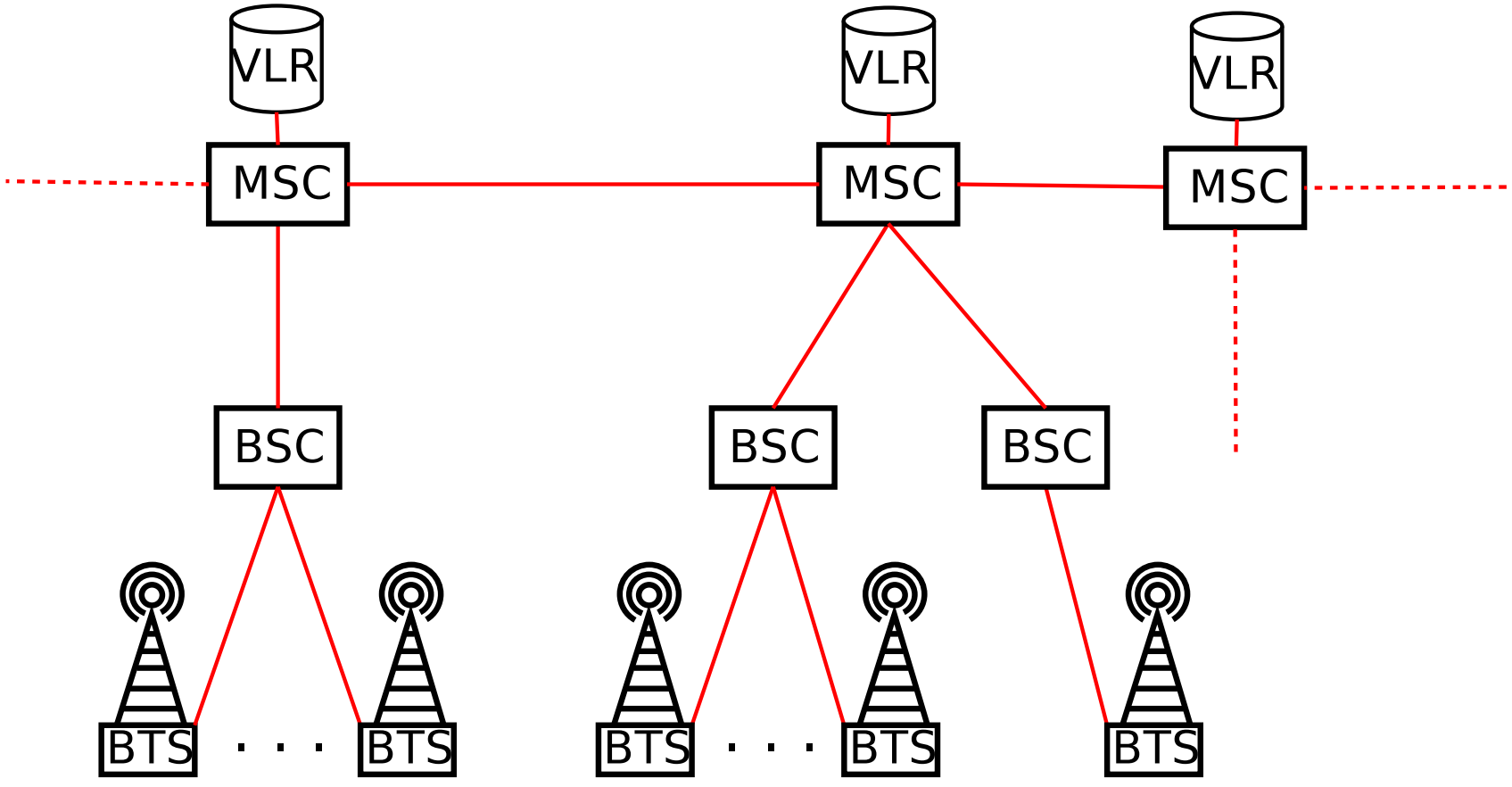
Phone call routing



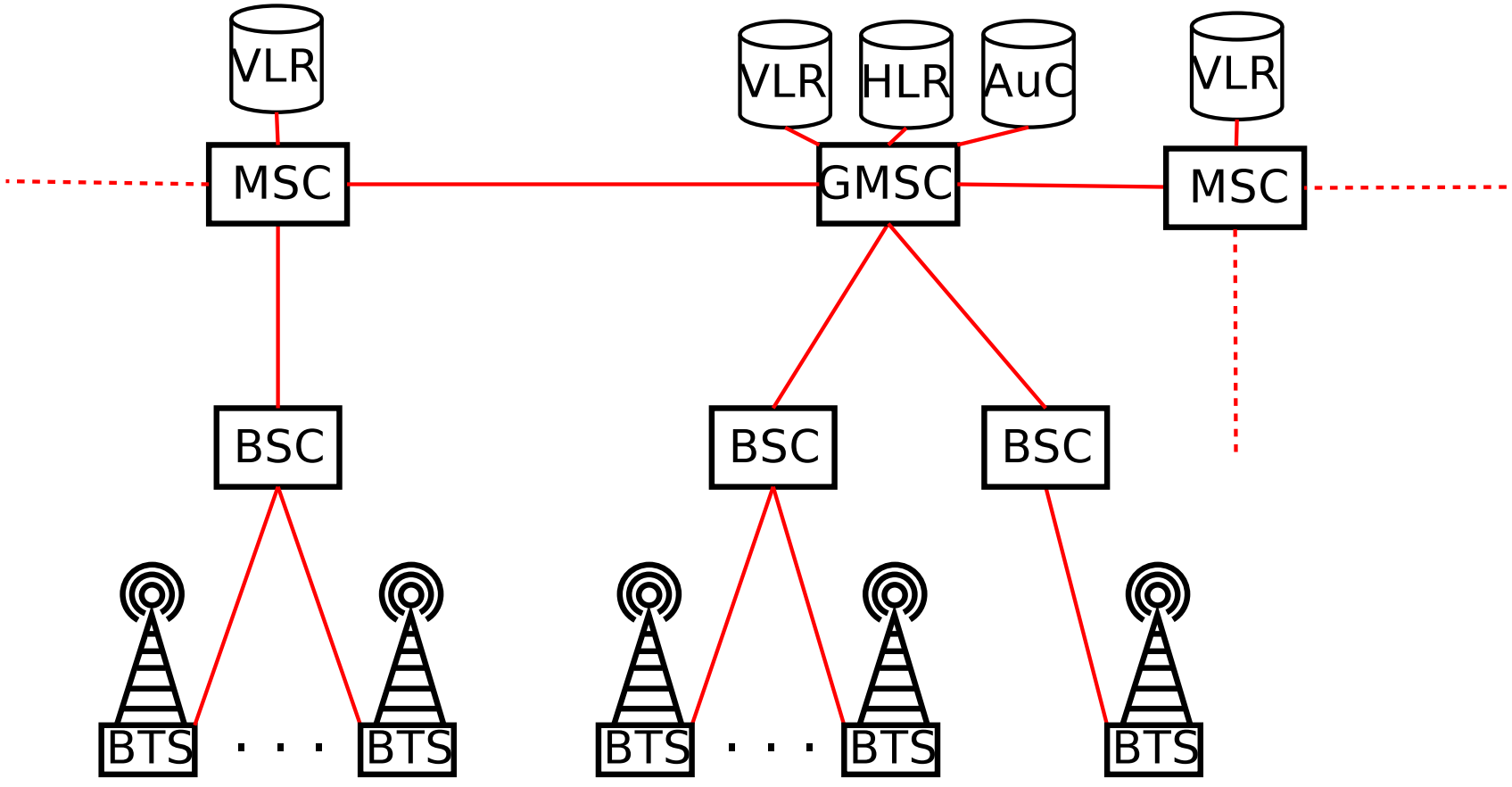
GSM system overview



GSM system overview



GSM system overview



Some important identifiers

- IMSI
- IMEI
- Phone number
- Secret key: Ki

GSM security

GSM security

- Authentication
  - A3
  - A8
  - COMP128
- Encryption
  - A5/0
  - A5/1
  - A5/2
  - A5/3

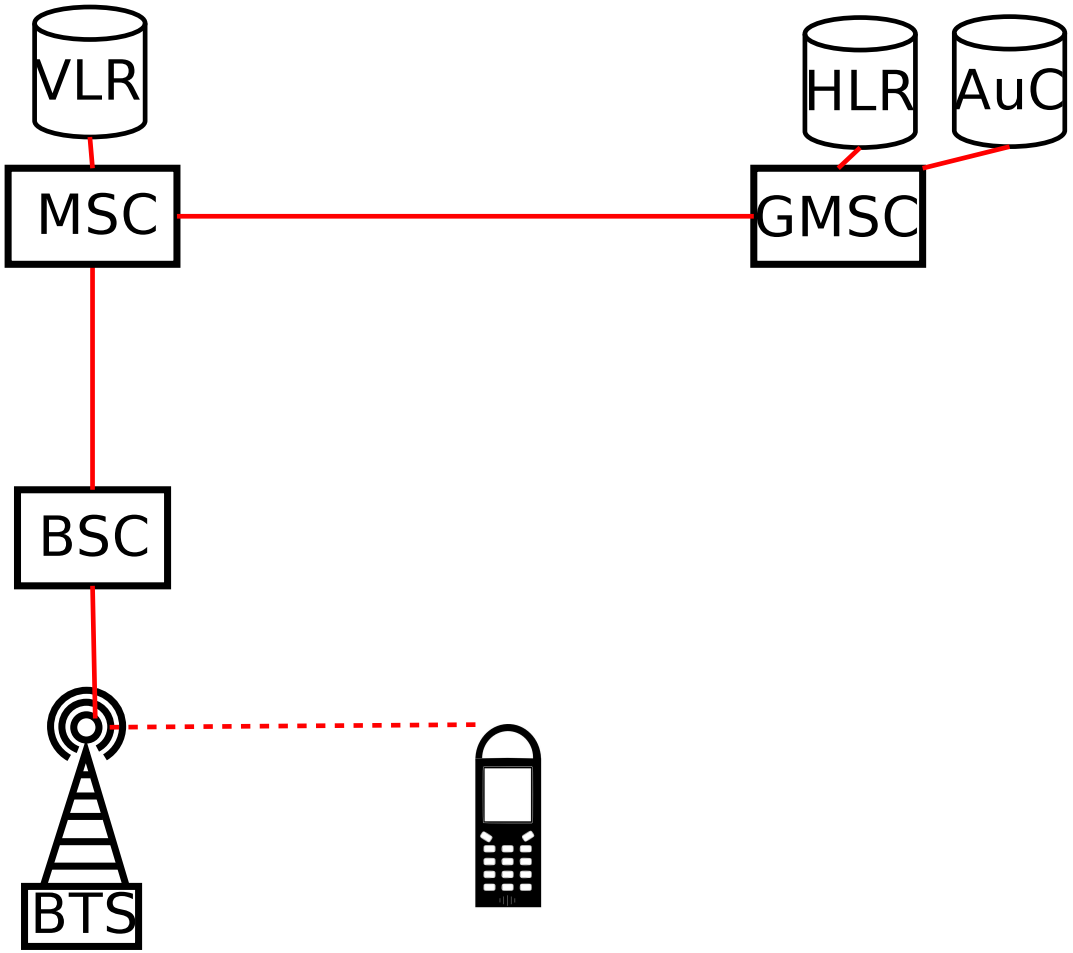
GSM security

- Authentication
  - A3
  - A8
  - COMP128
- Encryption
  - A5/0
  - A5/1
  - A5/2
  - A5/3

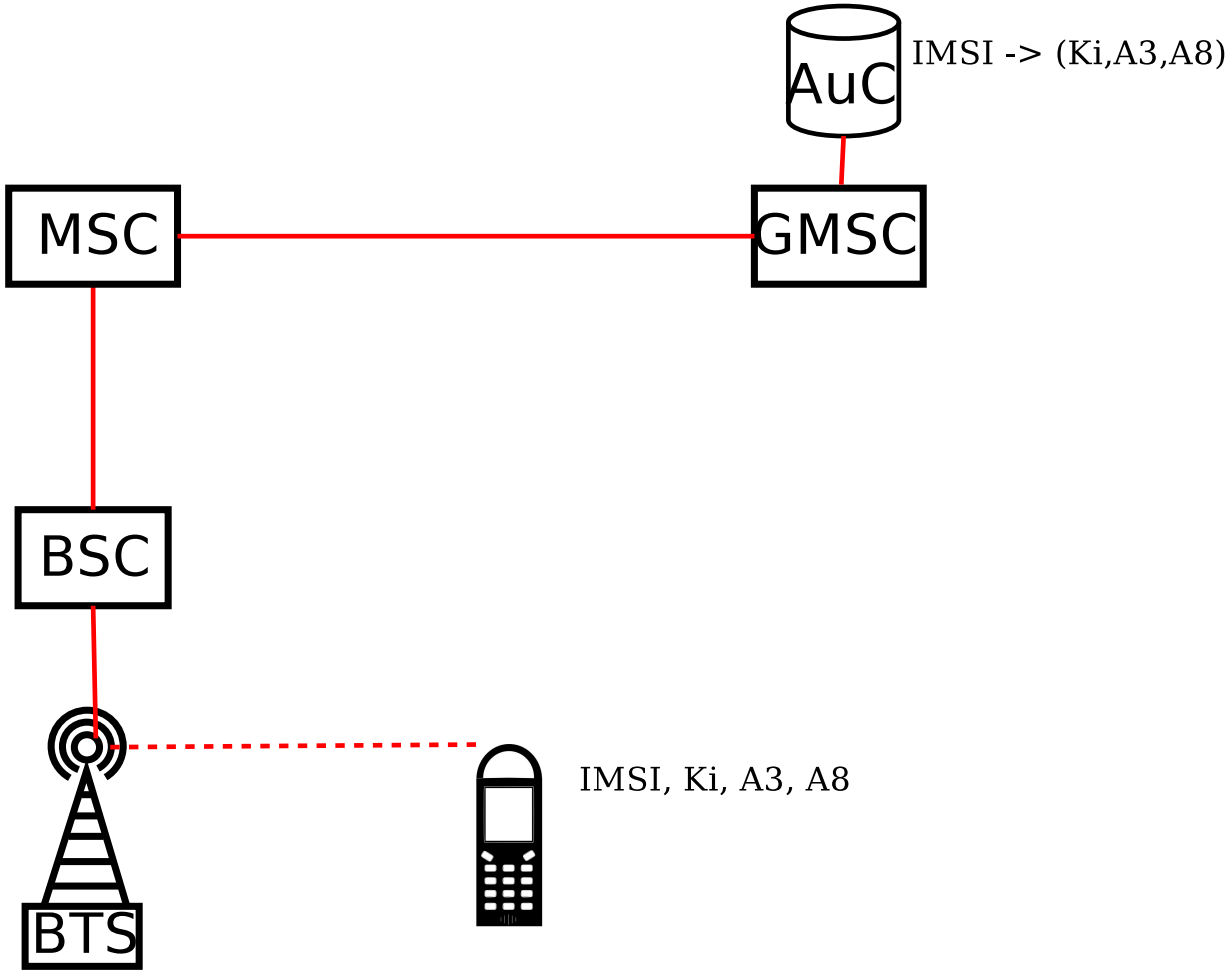
GSM security

- Authentication
  - A3
  - A8
  - COMP128
- Encryption
  - A5/0
  - A5/1
  - A5/2
  - A5/3

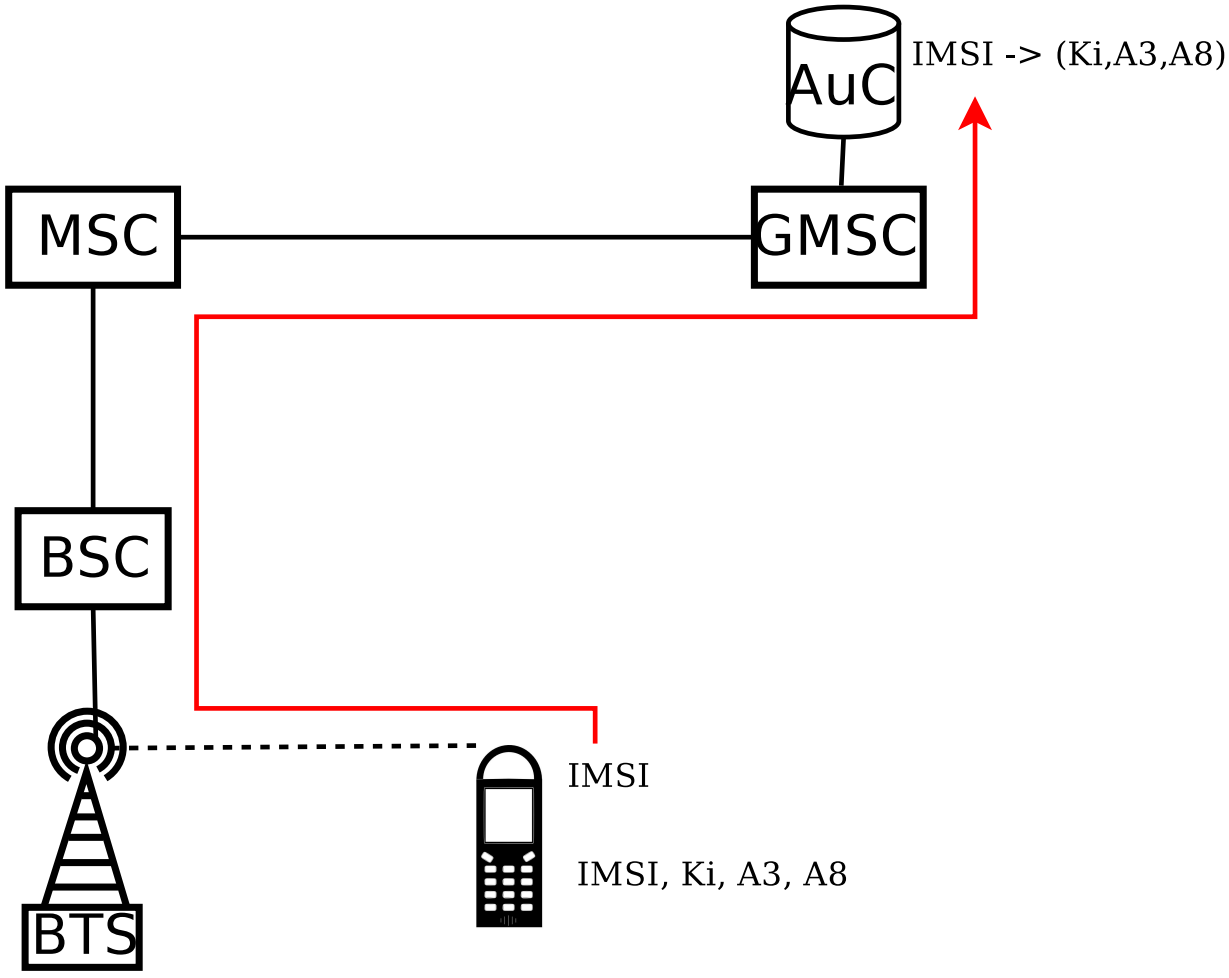
GSM authentication



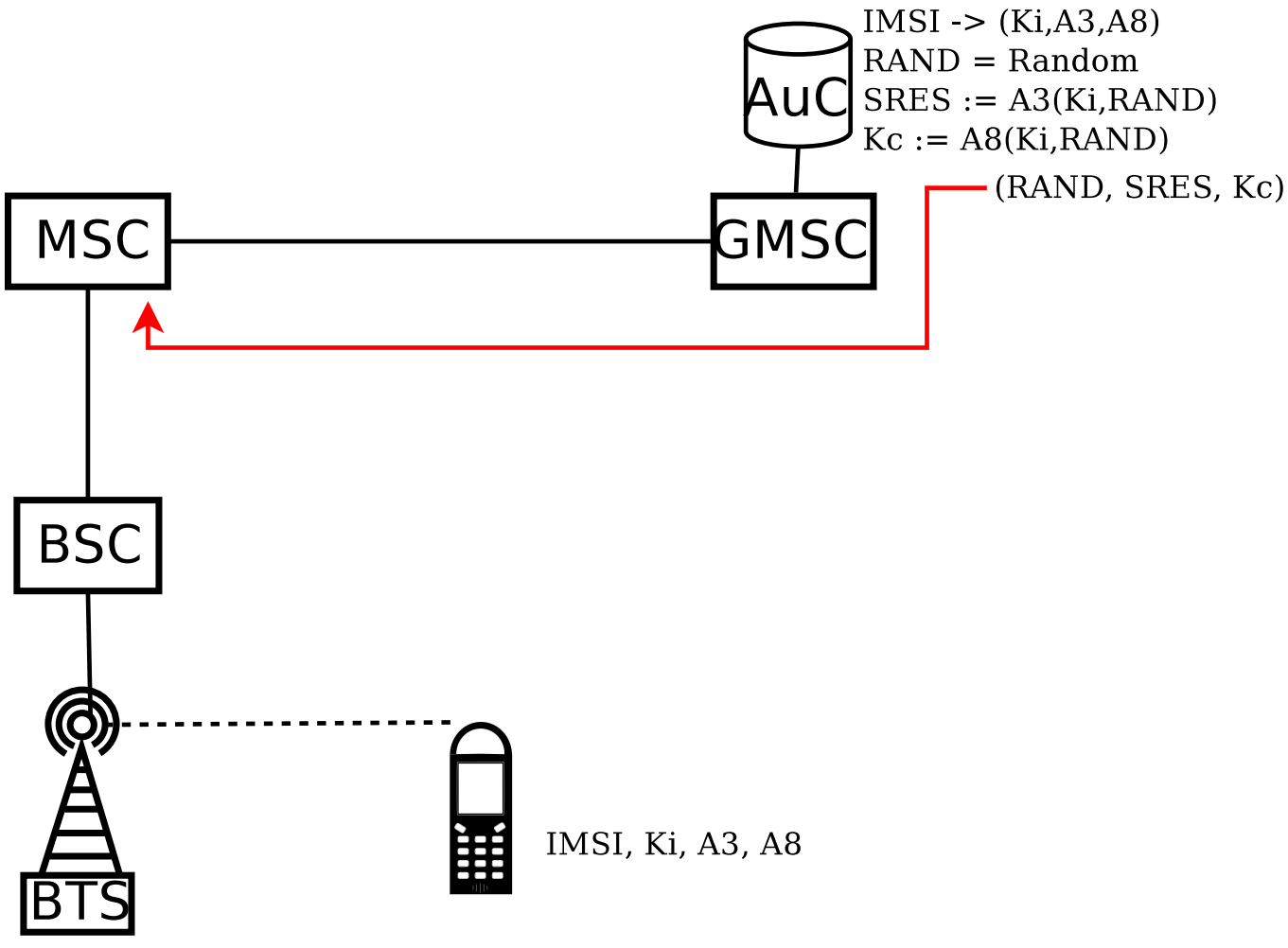
GSM authentication



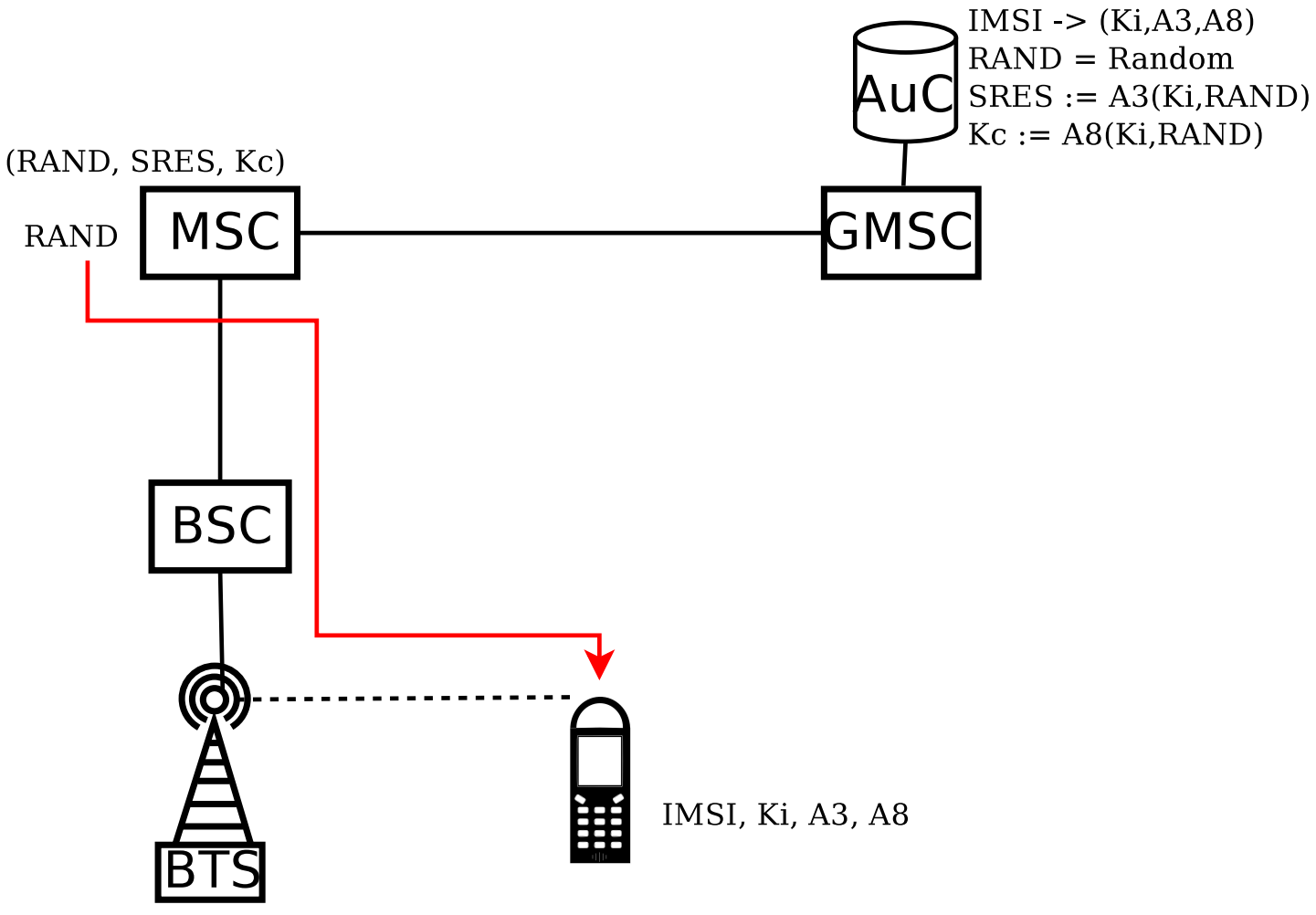
GSM authentication



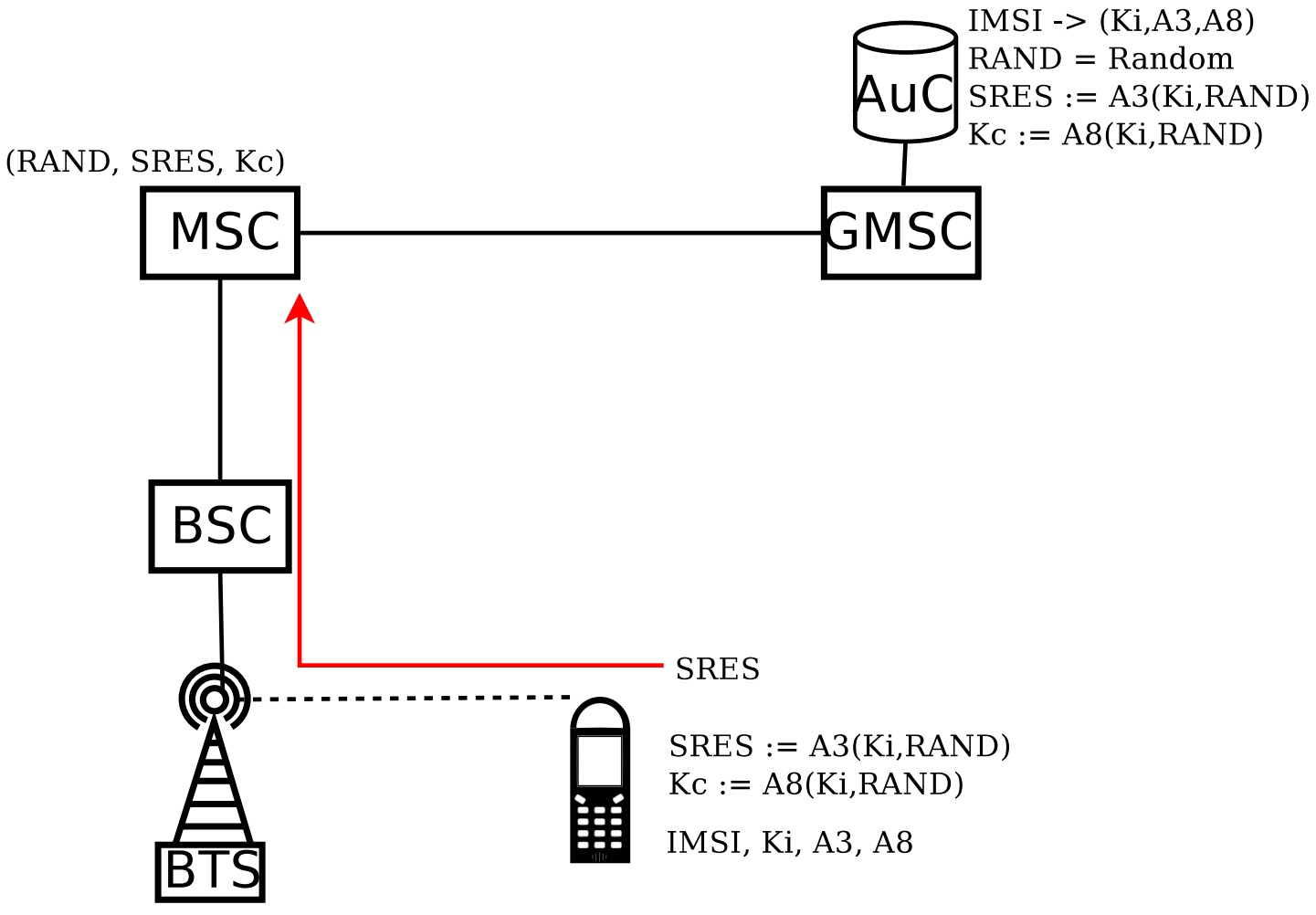
GSM authentication



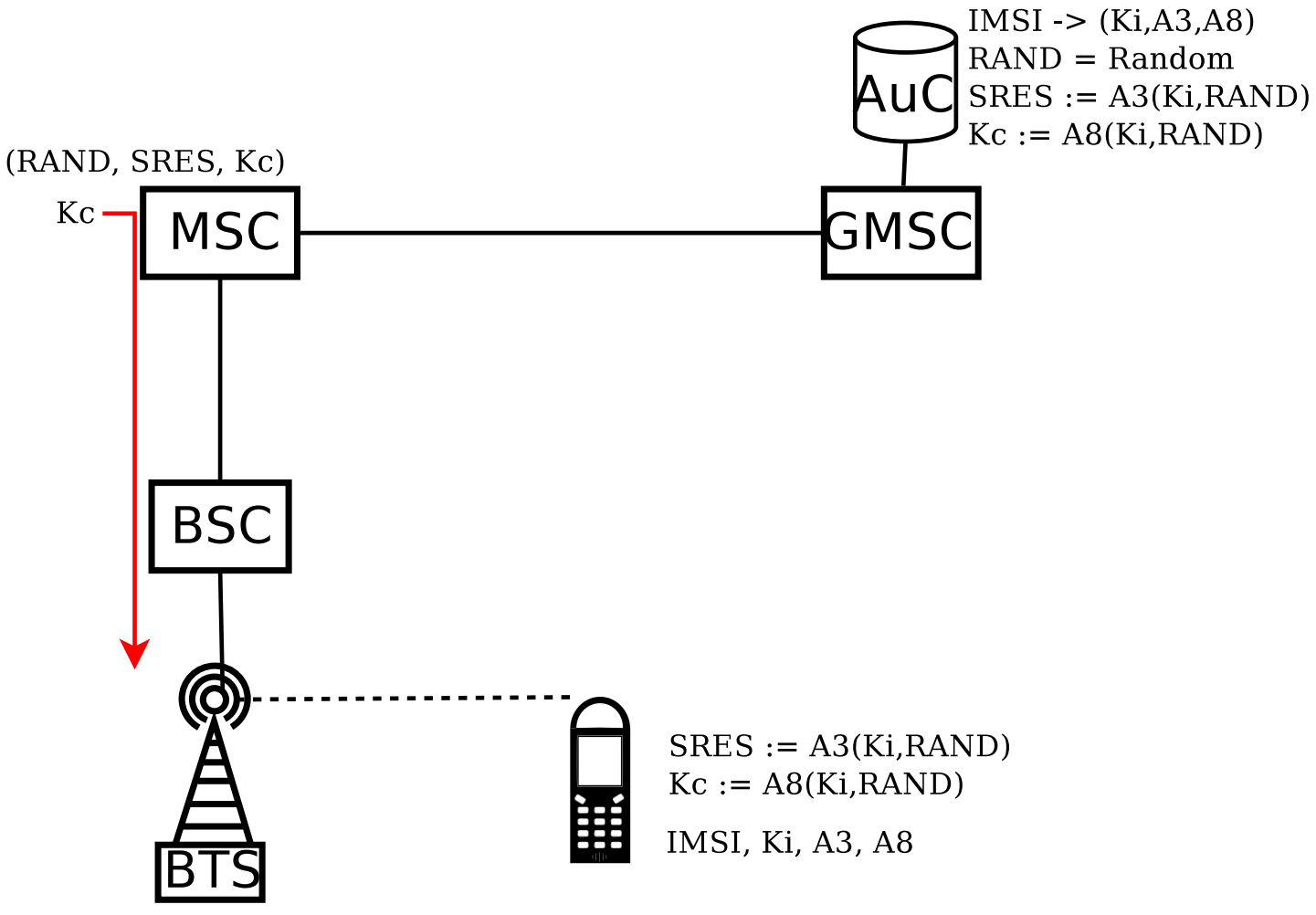
GSM authentication



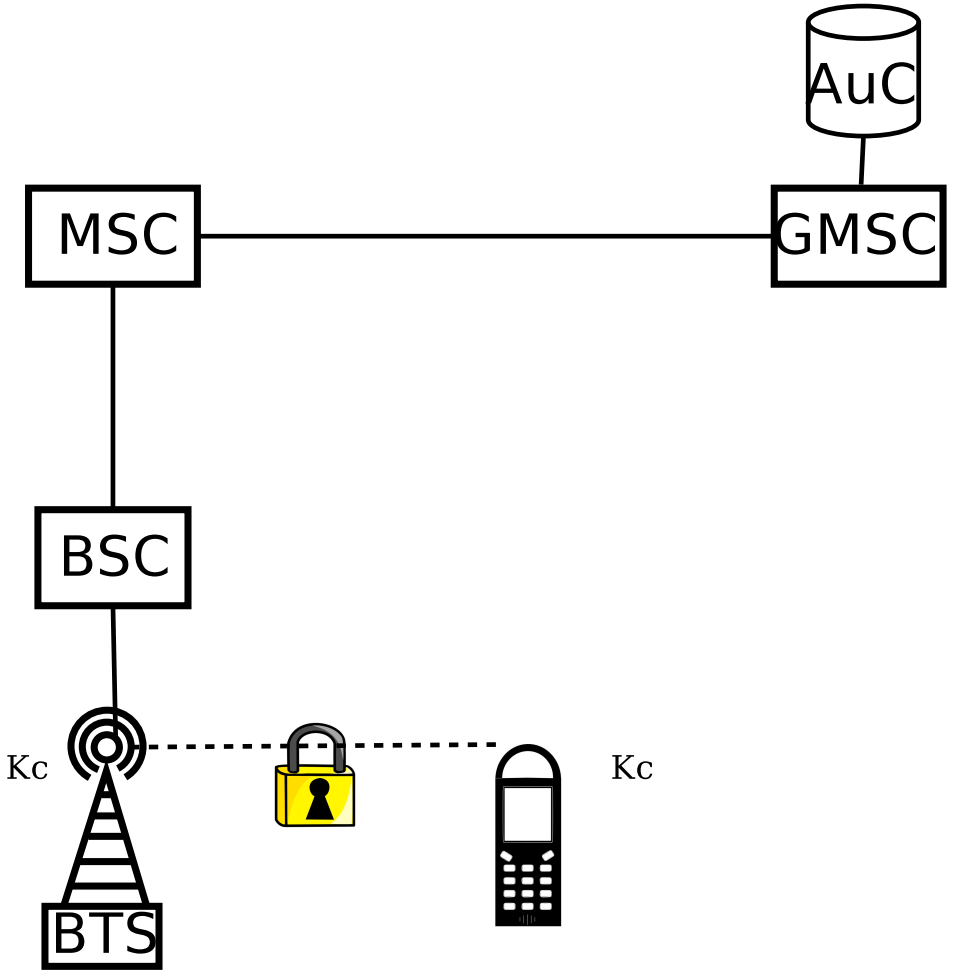
GSM authentication



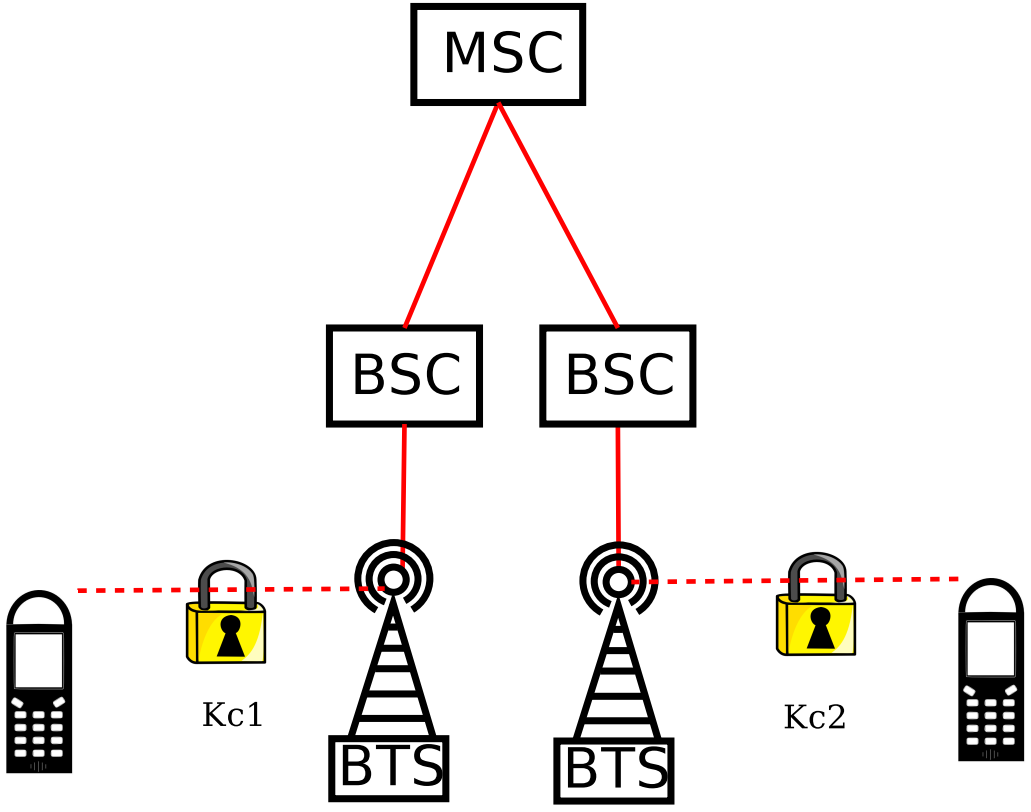
GSM authentication



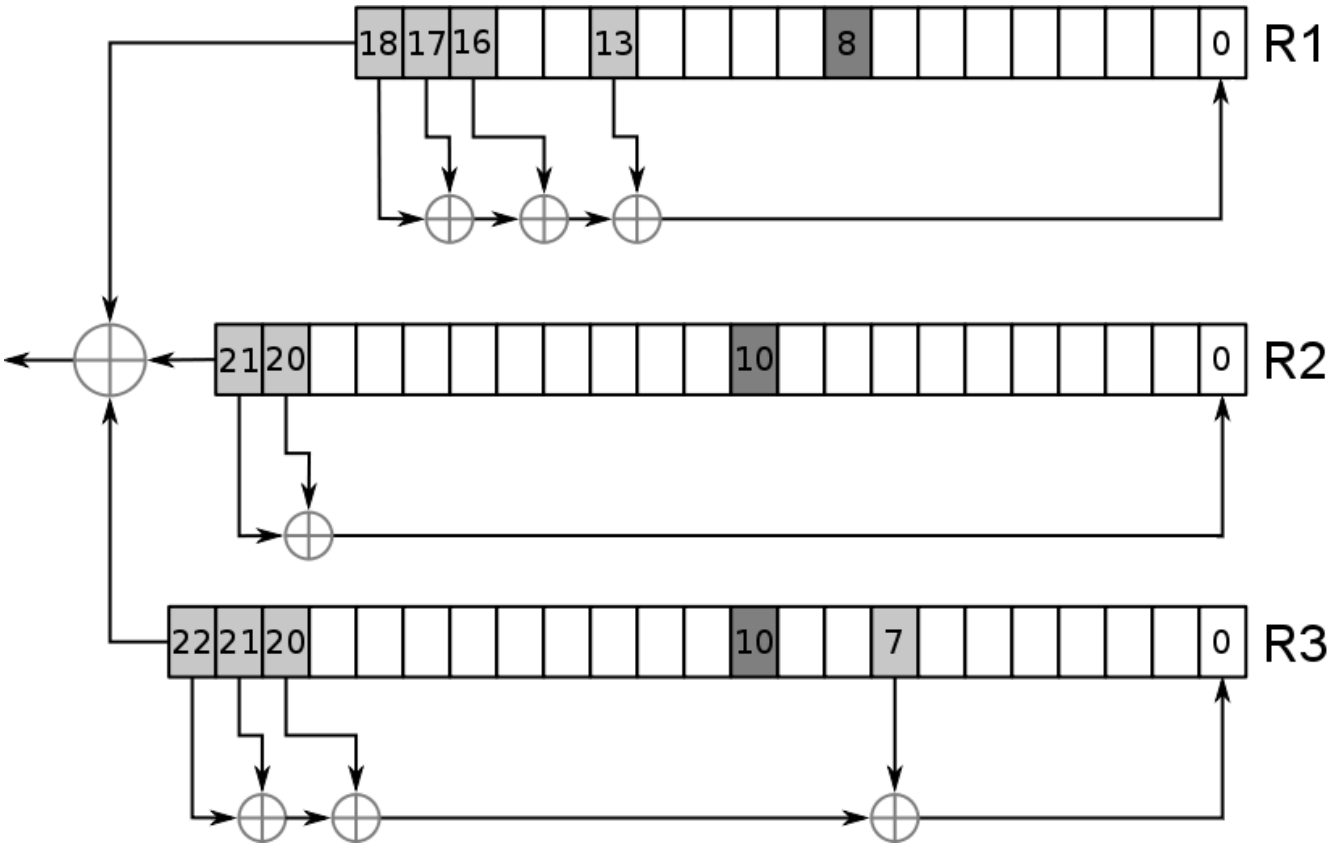
GSM Encryption



GSM Encryption



GSM Encryption



Attacks

Attack 1: Eavesdropping

Eavesdropping on GSM

1. Capture bursts
2. Decrypt captured bursts
3. Interpret decrypted bursts

3: Interpret decrypted bursts

You have several options here:

- GSMDecode (AirProbe)
- WireShark
- OpenBTS / OpenBSC

2: Decrypt captured bursts

Release the Kraken!

Breaking A5/1

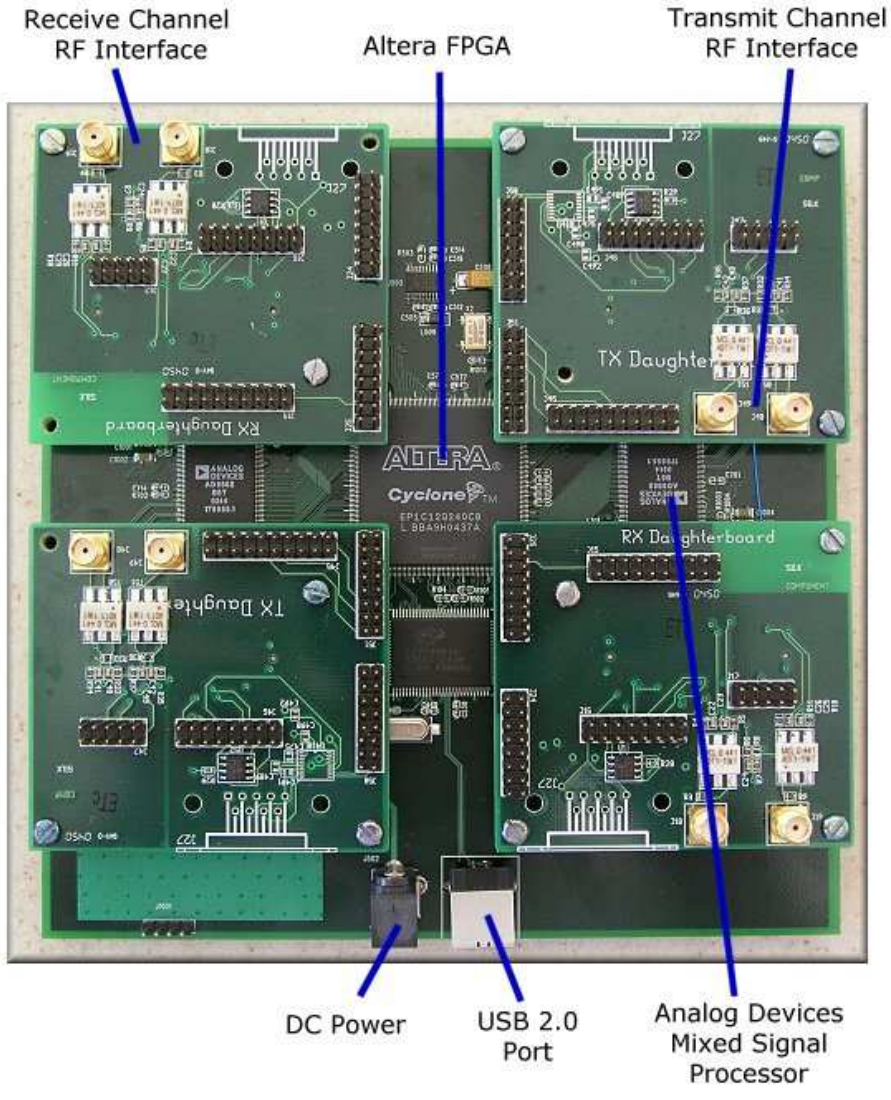
- Reverse engineered in 1994
- Academic breaks
- Time-Memory-Trade-Off attacks
- Currently:
  - Berlin set & Kraken

Using Kraken

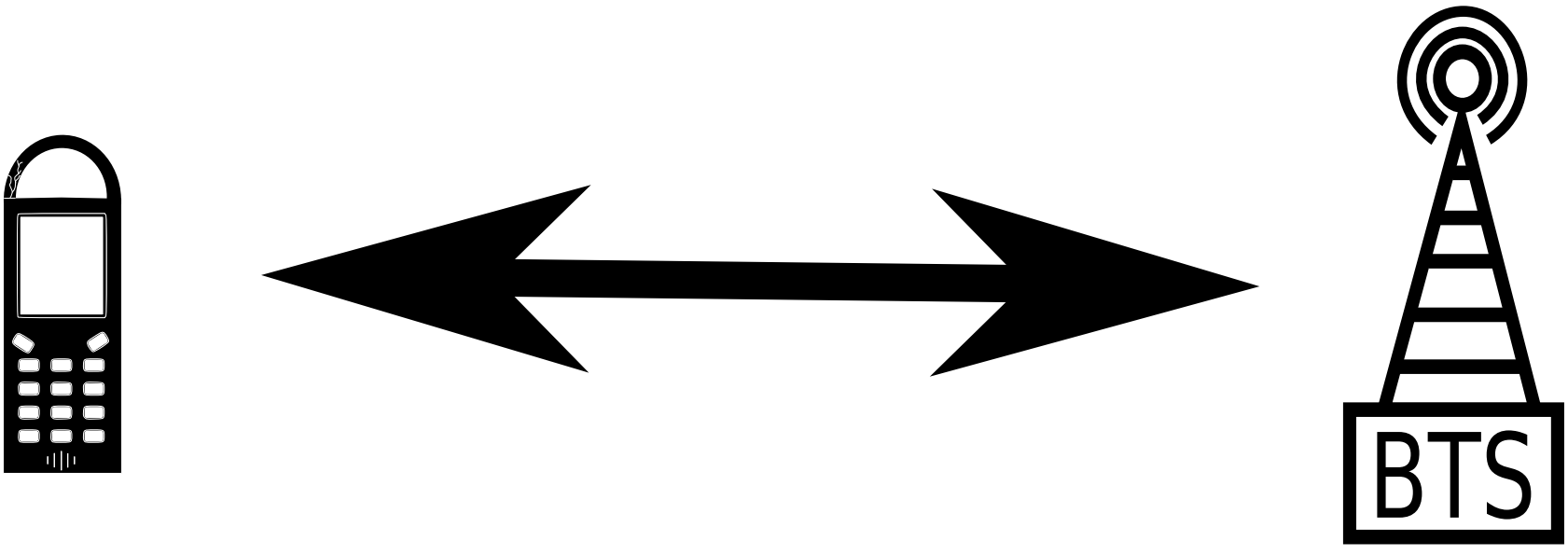
1. Capture a burst
2. “Guess” contents
3. Compute keystream
4. Look-up corresponding session key

1: Capture burst

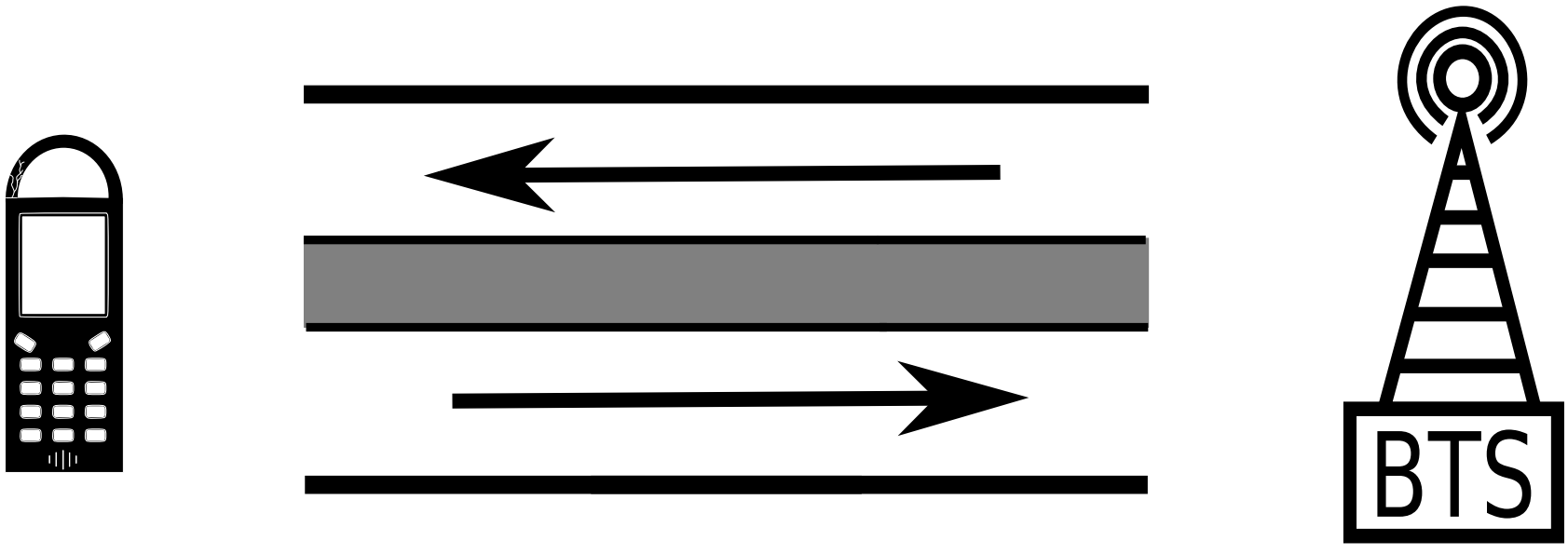
USRP + GNU Radio + AirProbe



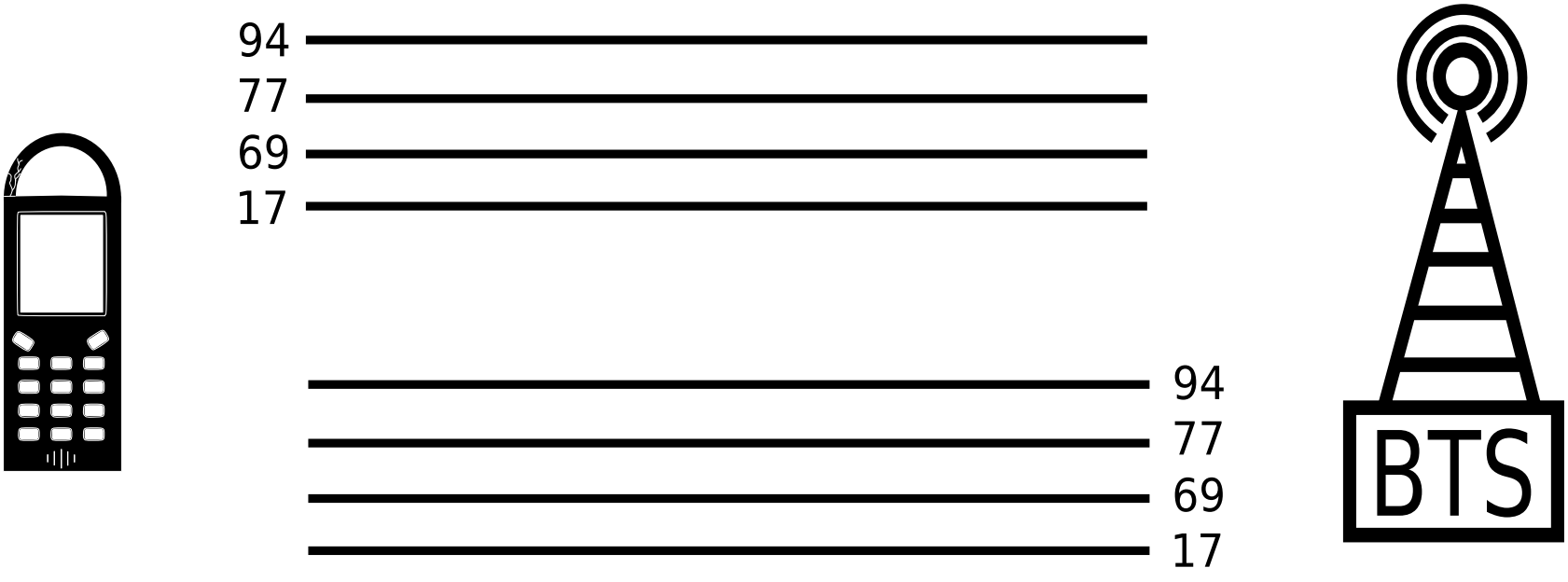
The Um interface



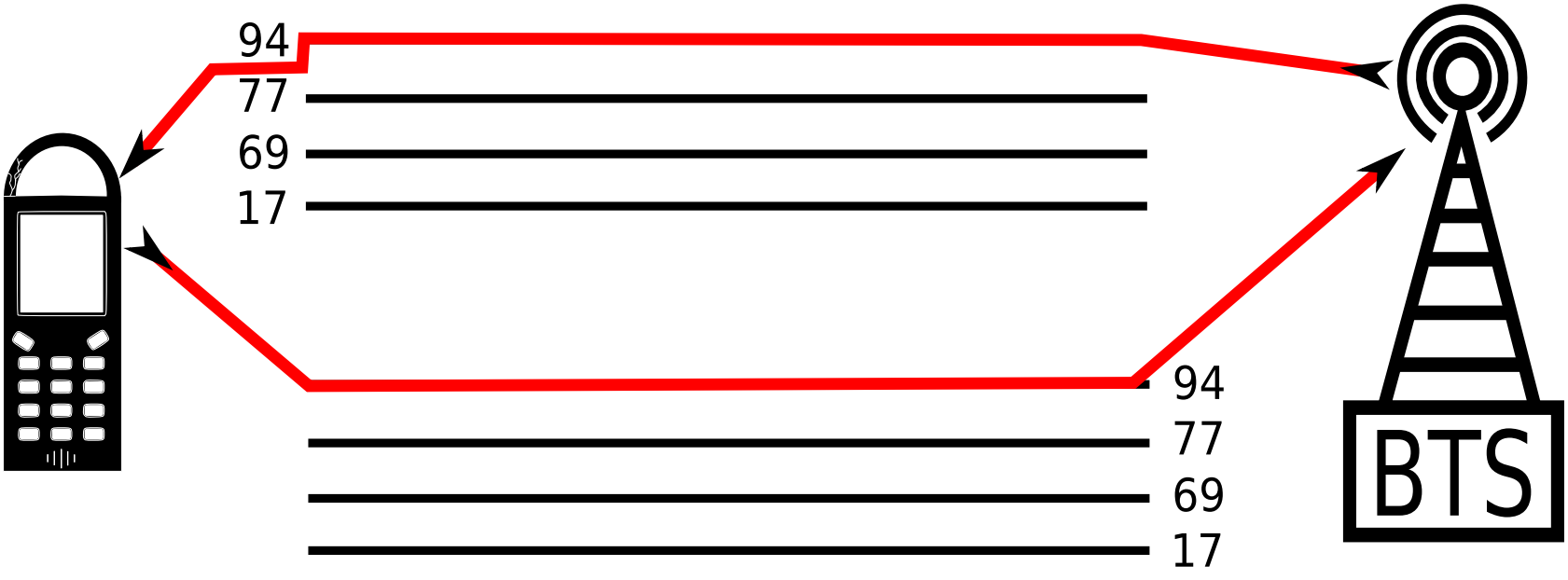
Frequency band



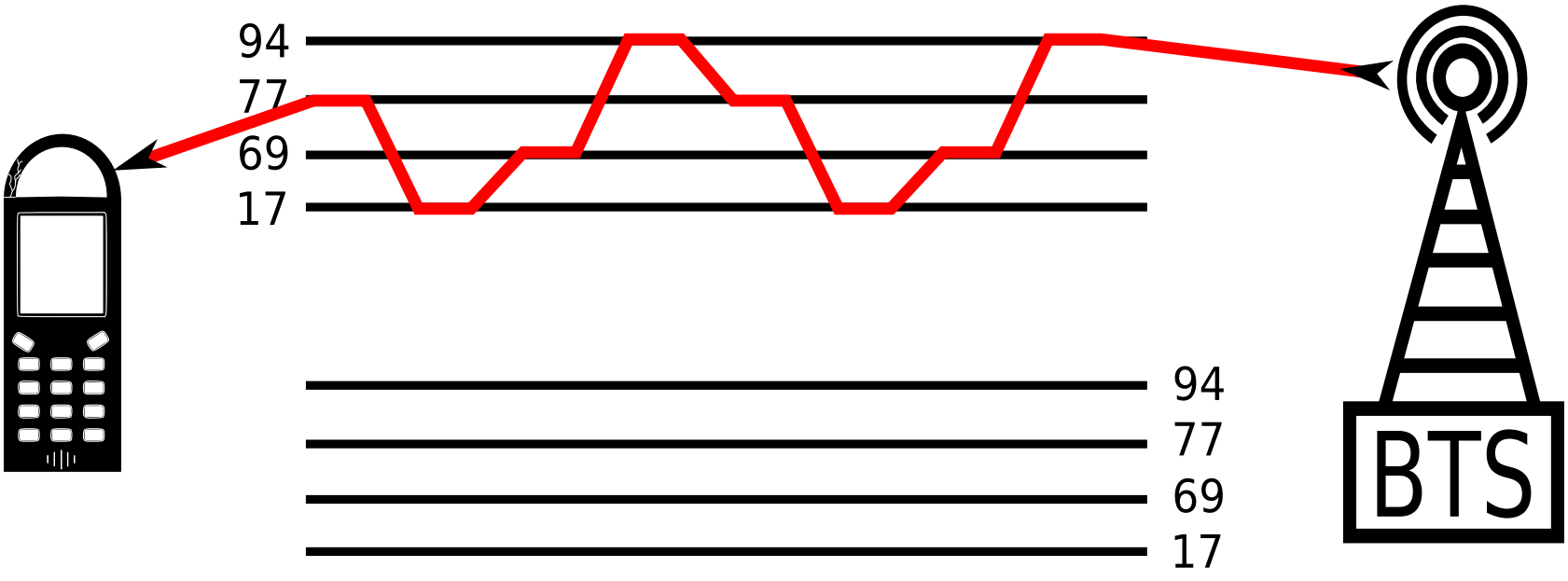
An example cell



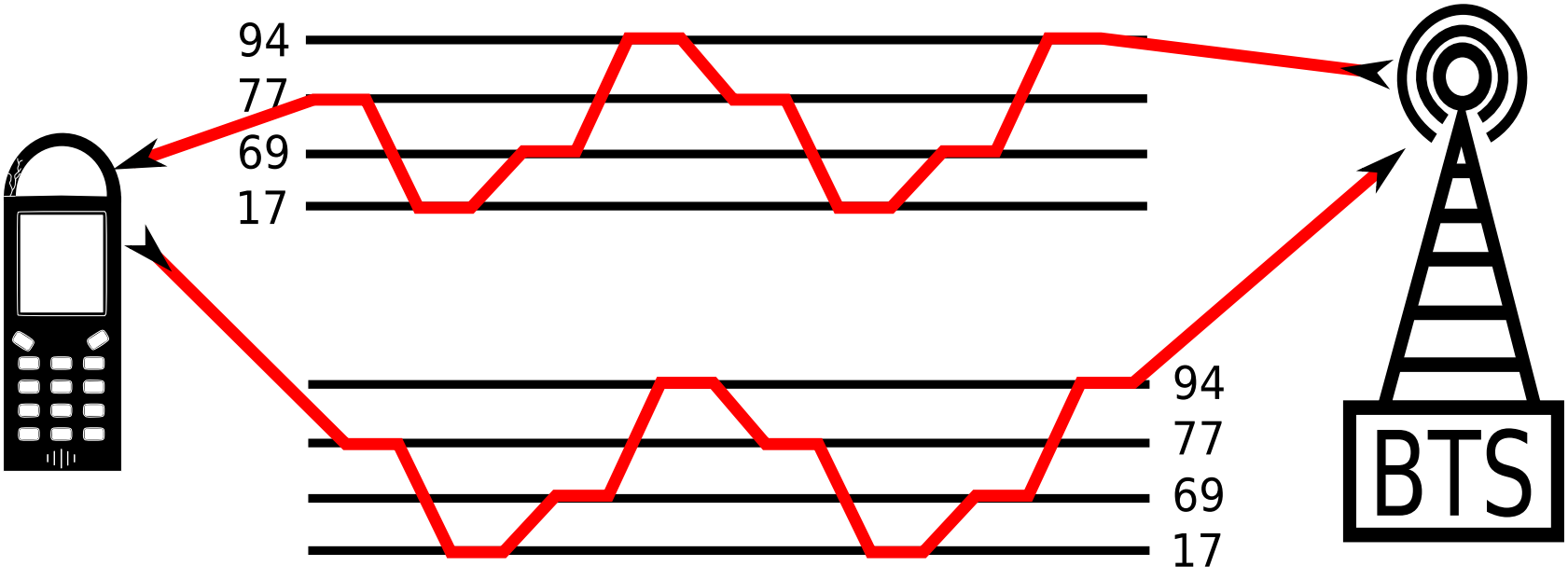
No Frequency hopping



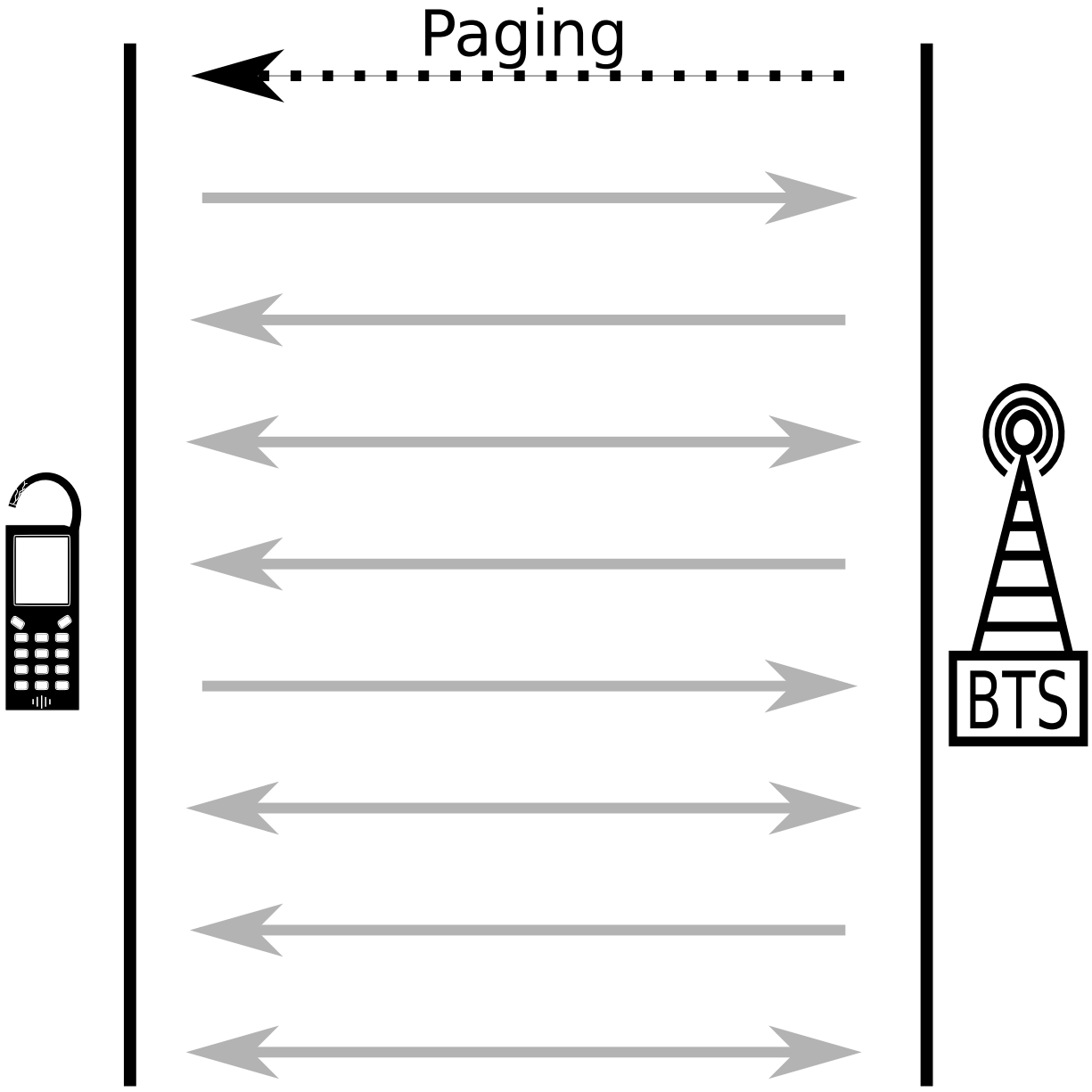
Frequency hopping



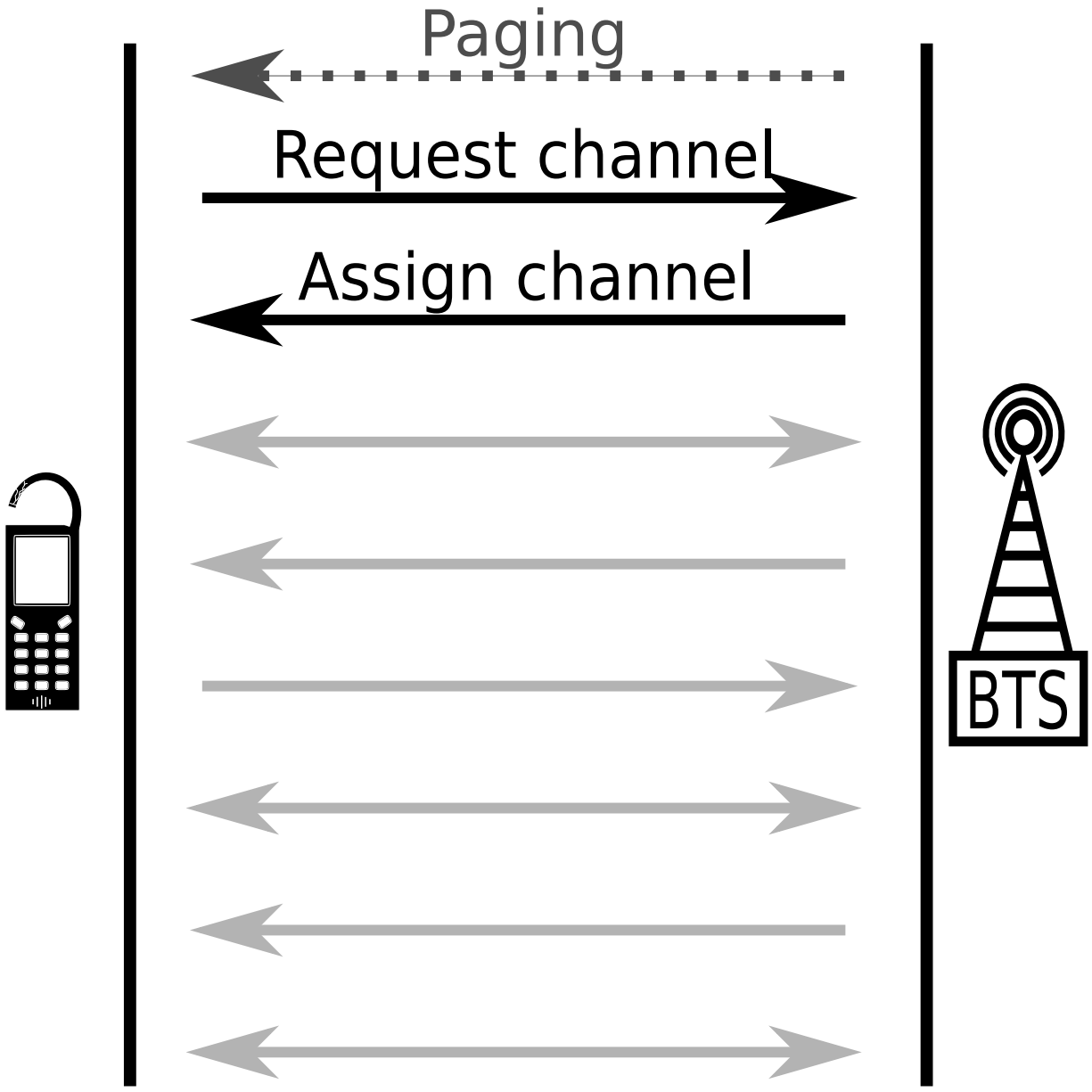
Frequency hopping



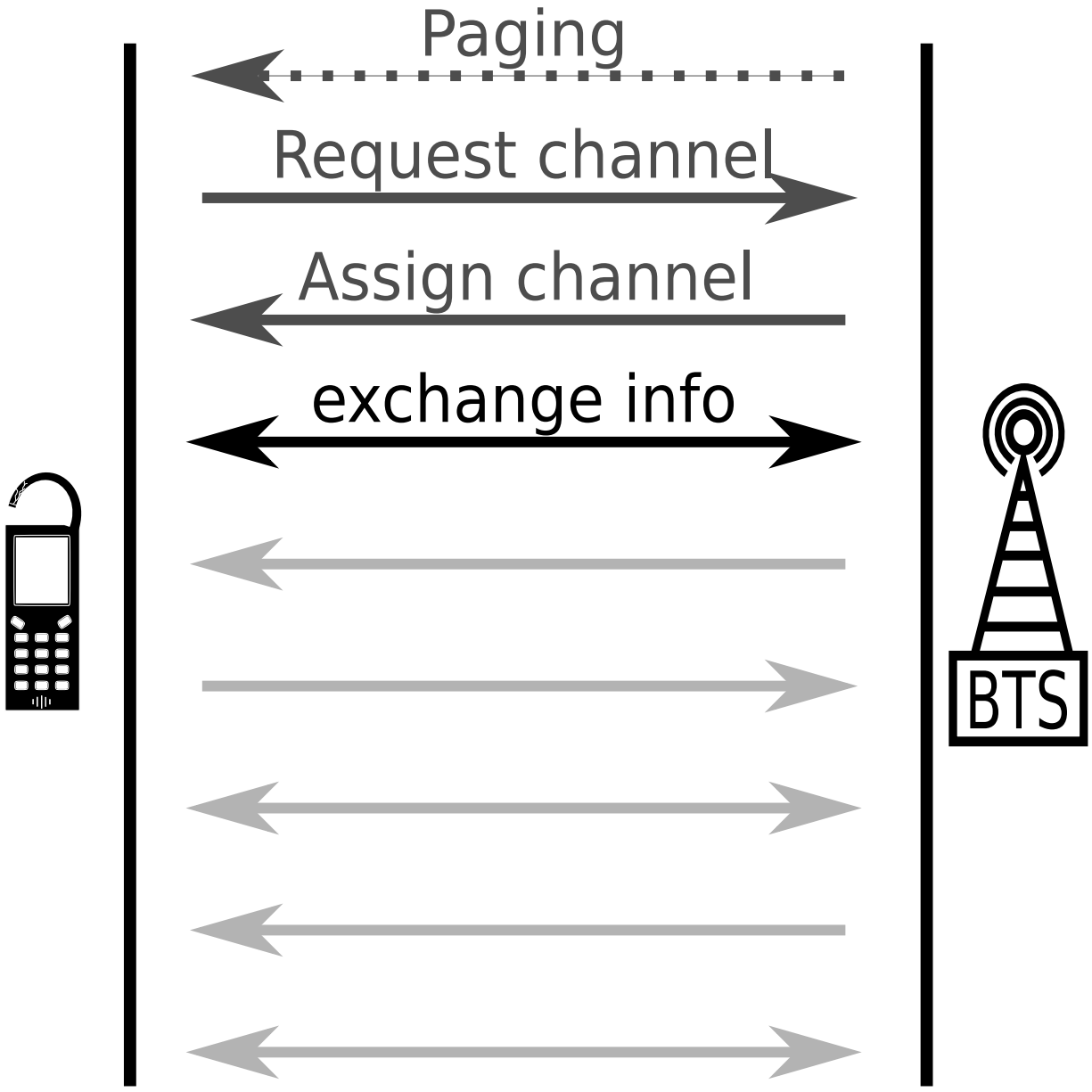
Message Sequence



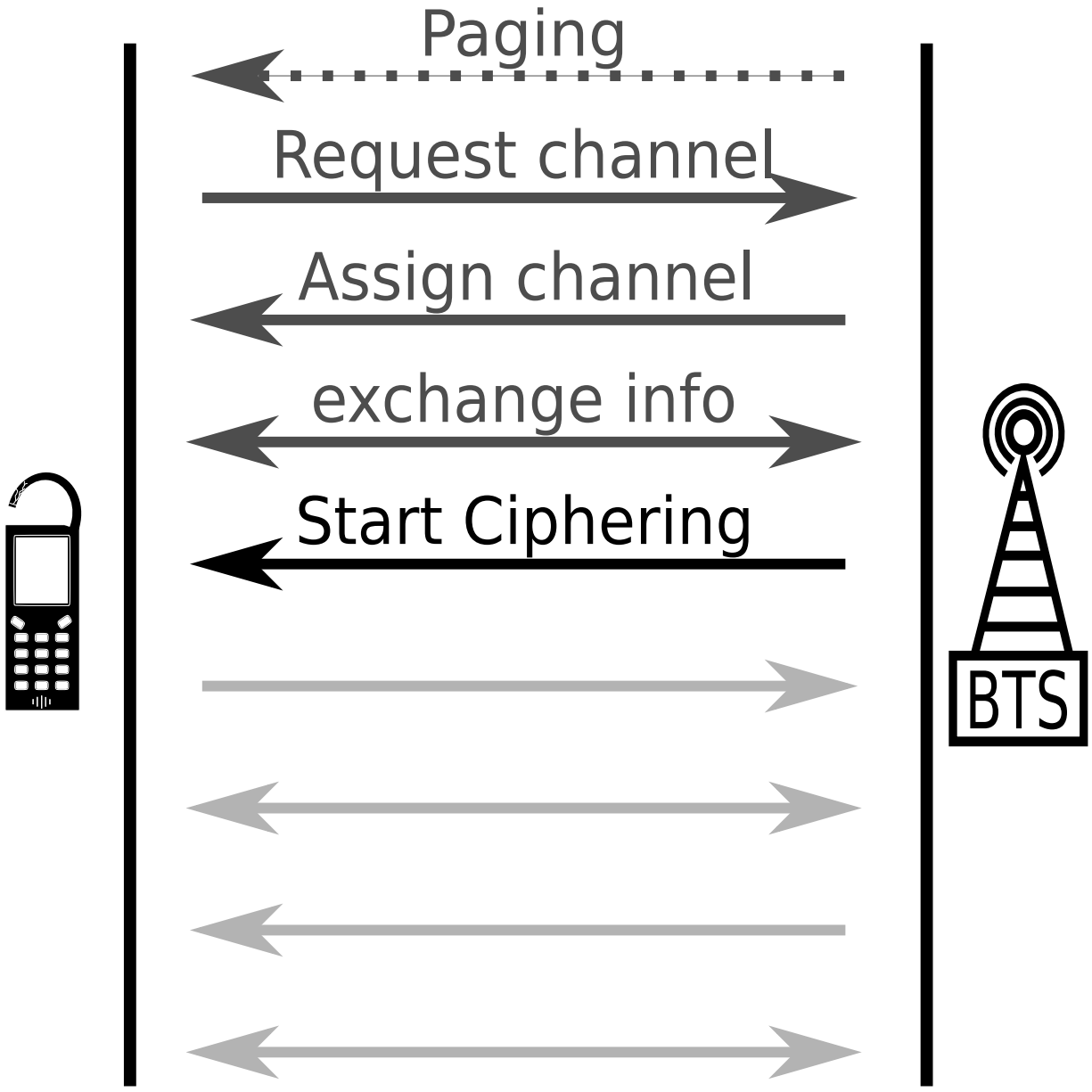
Message Sequence



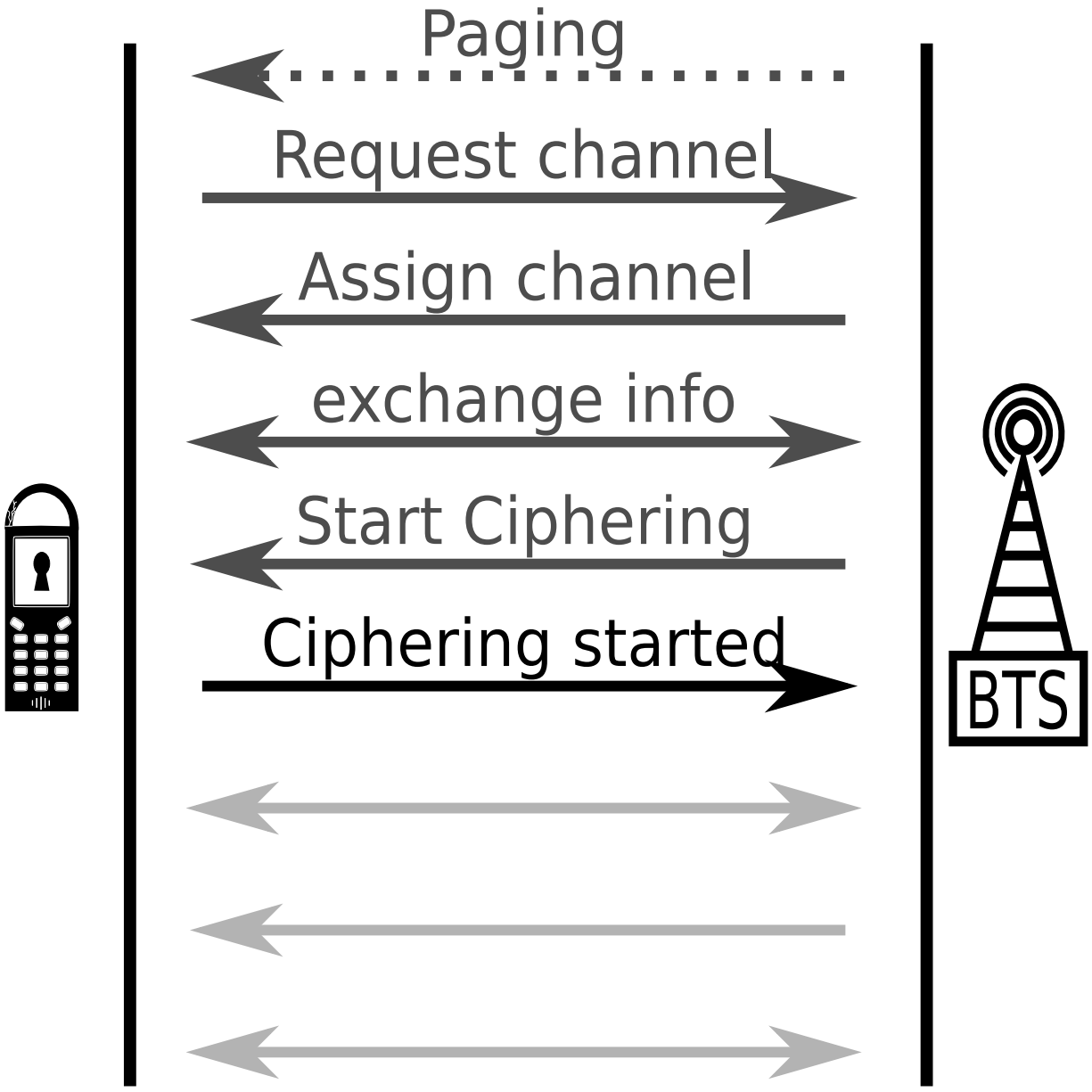
Message Sequence



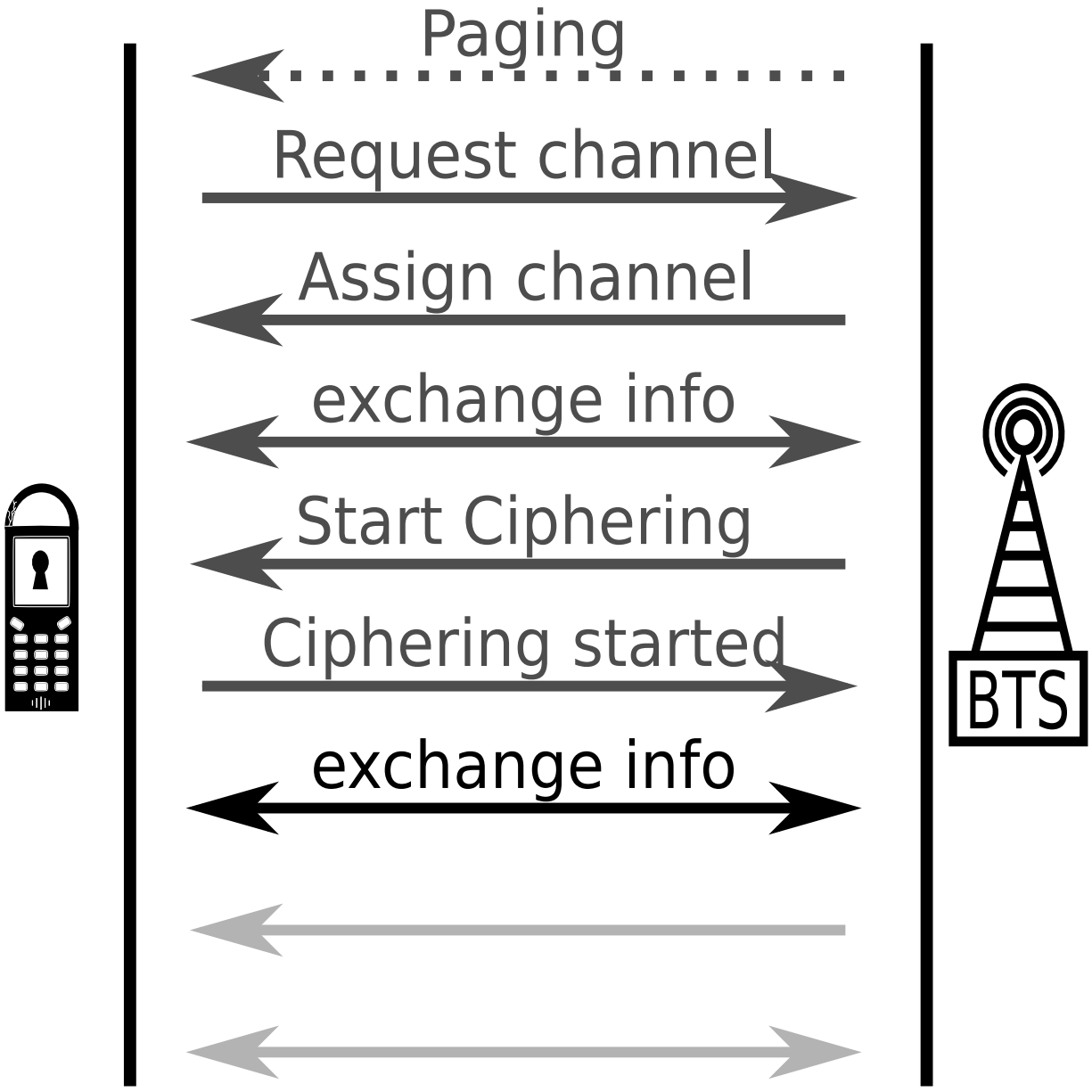
Message Sequence



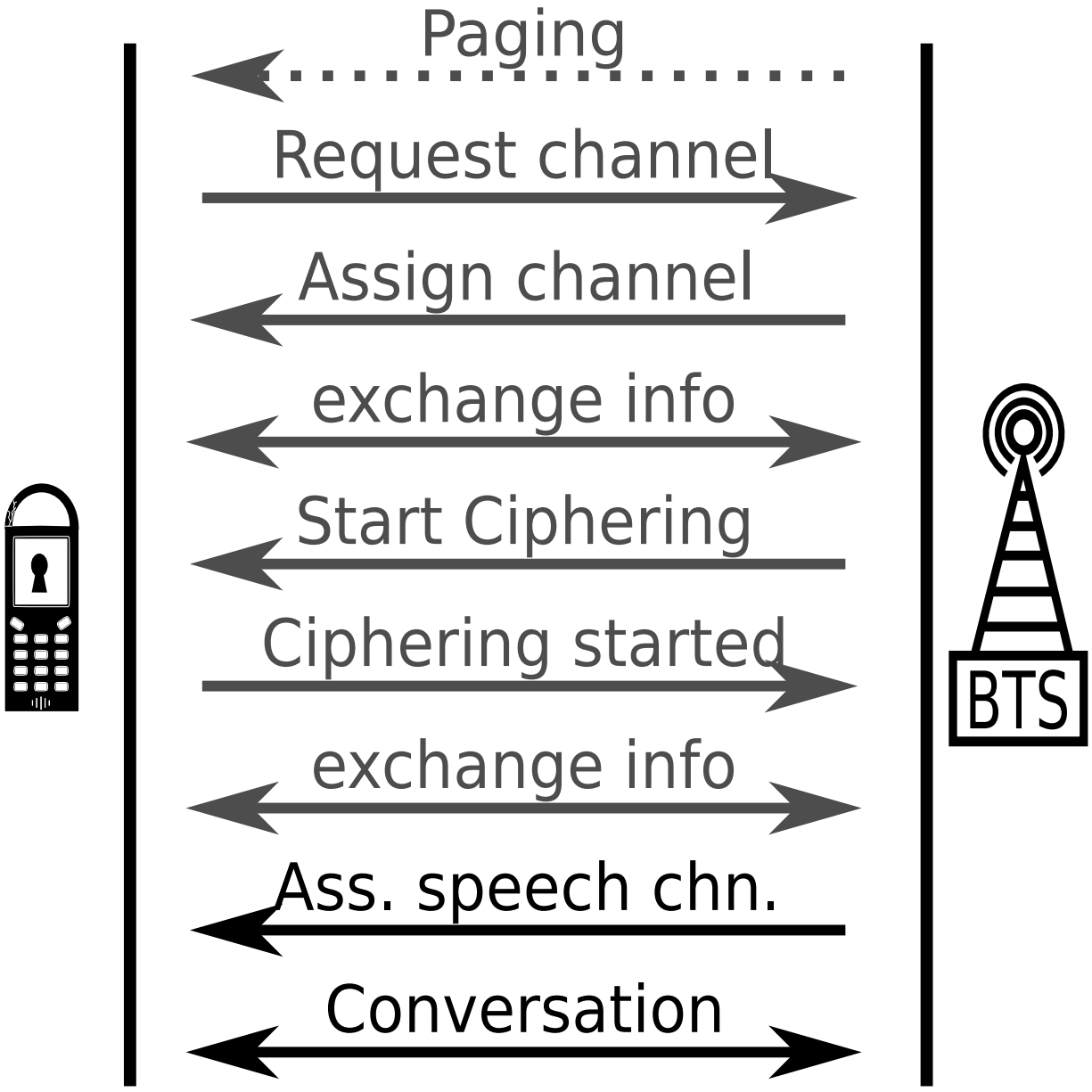
Message Sequence



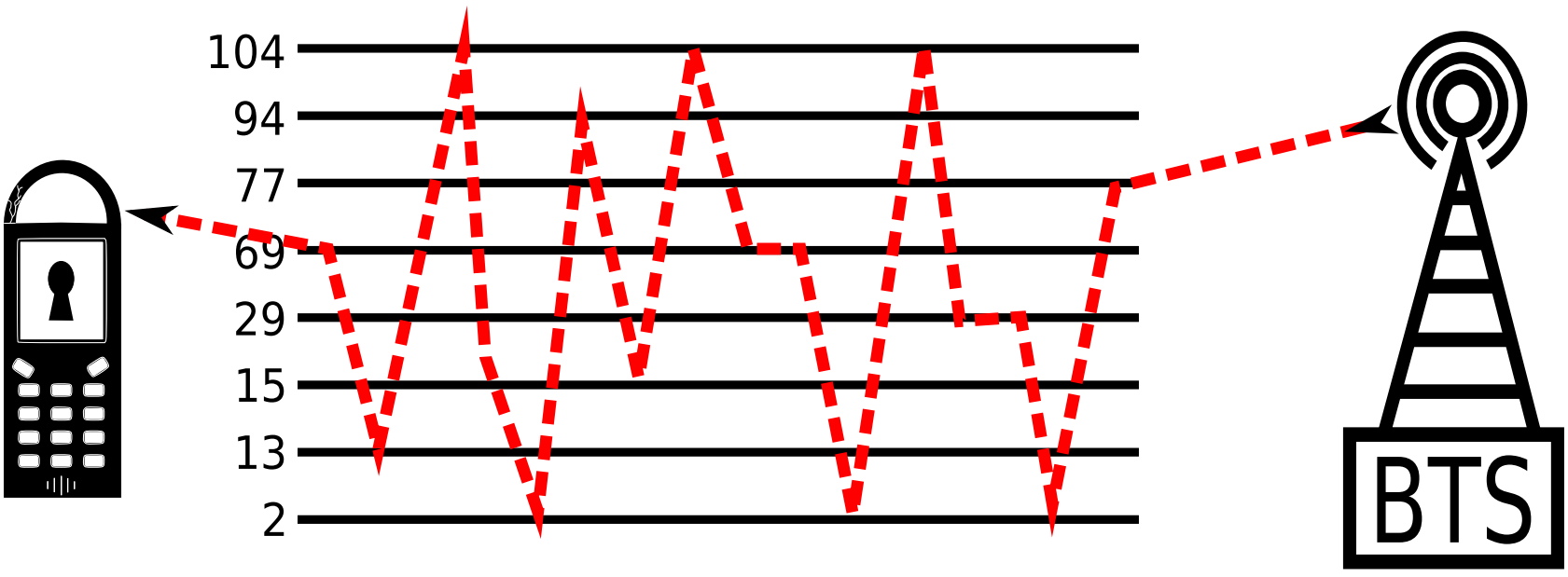
Message Sequence



Message Sequence

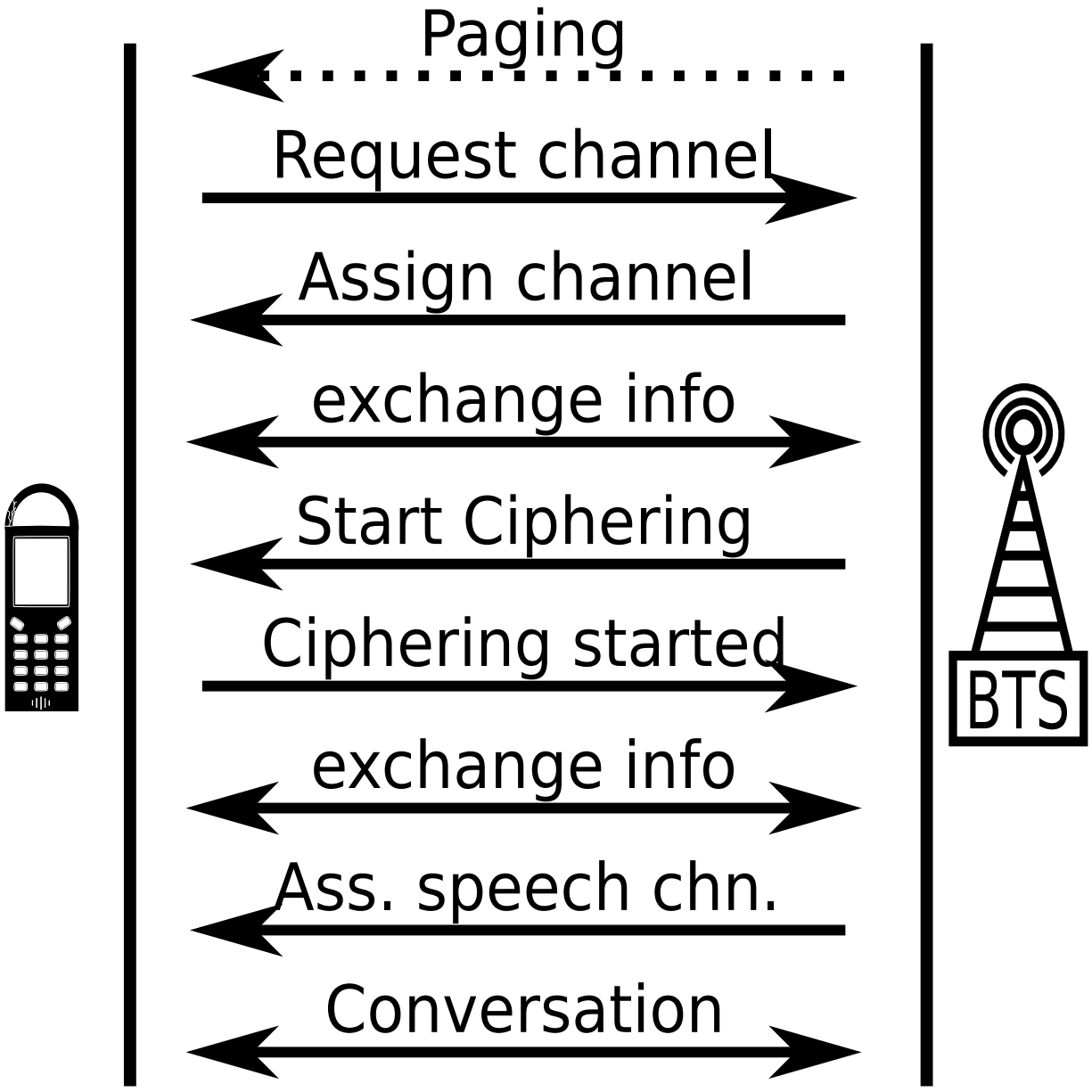


Hopping Problem

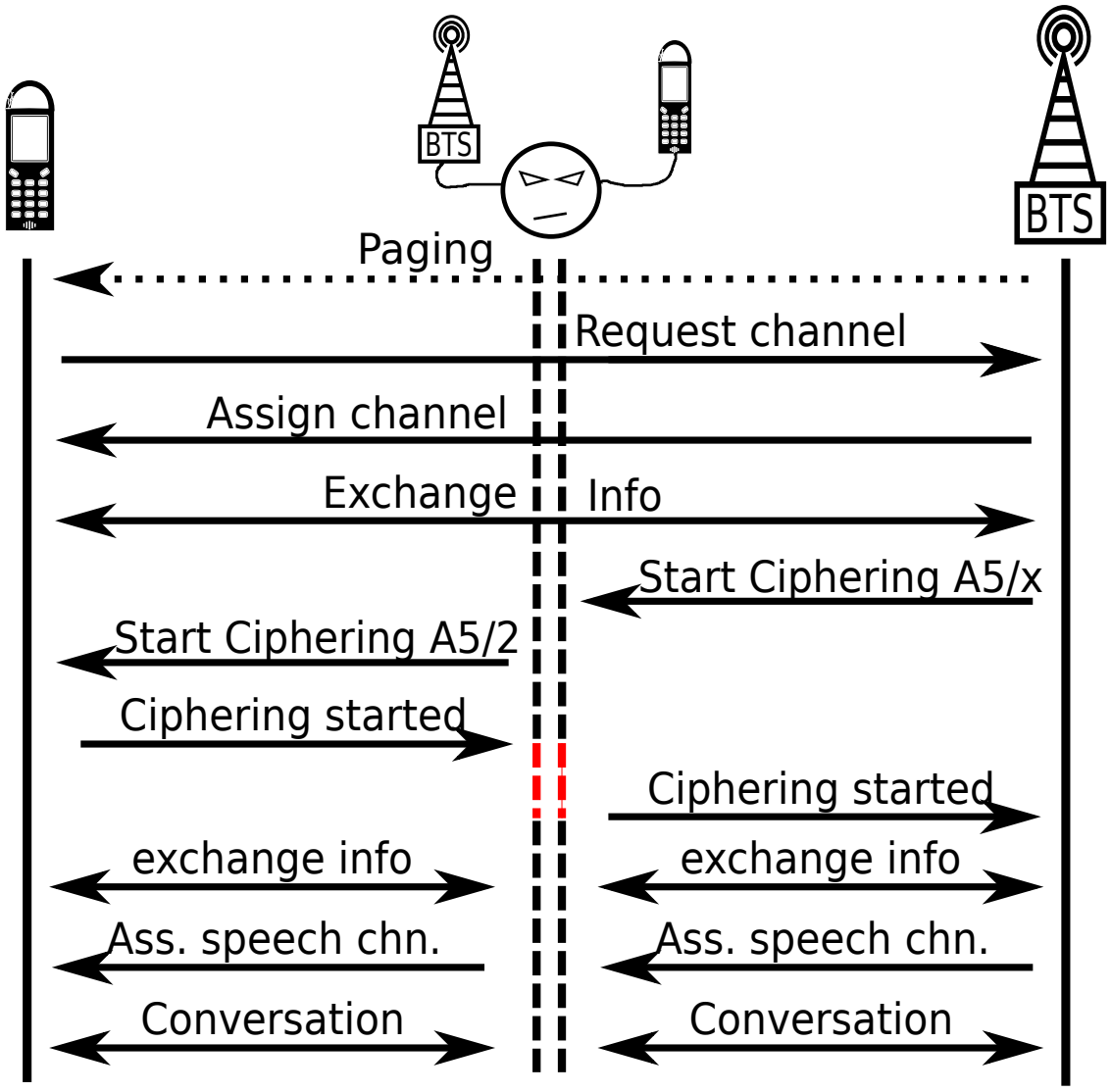


Attack 2: the MITM attack

The Man-In-The-Middle Attack



The Man-In-The-Middle Attack



The Man-In-The-Middle Attack

Ingredients:

- BTS: OpenBTS / OpenBSC
- Phone: OsmocomBB

Problems:

- Hopping problem
- Time window
- Detectable

MITM the easy way

Just link OpenBTS to Asterisk

Downsides:

- No incoming calls
- Calling number obscured

Upside:

- It already works

MITM the easy way

Just link OpenBTS to Asterisk

Downsides:

- No incoming calls
- Calling number obscured

Upside:

- It already works

Yet another way

A sort of hybrid attack between MITM and eavesdropping

1. Capture challenge
2. Capture conversation
3. Fake BTS attack with challenge

Some other attacks

Other attacks

- IMSI catchers
- Attacks on other parts of the network
- Nokia 1100
- Locations revealed
- DoS attacks

There’s hope still

GSM was 2G

3G uses mutual authentication

4G might use AES

What can you do now?

GSM will be around for a long time.

- Use **solely** 3G
- Use crypto solutions

Conclusions

Conclusion

- Eavesdropping, full-MITM and hybrid still need work
- Easy-MITM works
- Many other attacks are possible

....Besides

The weakest link is probably your phone!

See The Monkey Steals the Berries

....Besides

The weakest link is probably your phone!

See The Monkey Steals the Berries

Questions

References

USRP www.ettus.com
GNU Radio http://gnuradio.org/
OpenBTS http://openbts.sourceforge.net/
OpenBSC
http://openbsc.osmocom.org/trac/wiki/OpenBSC
AirProbe
https://svn.berlin.ccc.de/projects/airprobe/wiki
A5/1, Kraken http://www.reflextor.com/trac/a51
OsmocomBB http://bb.osmocom.org/trac/