Berlin Institute of Technology

FG Security in Telecommunications

© Weiss

Let Me Answer That for You!

adventures in mobile paging

29th Chaos Communication Congress (29c3)

Nico Golde, Kevin Redon, Hamburg, Dec 28th 2012

{nico,kredon}@sec.t-labs.tu-berlin.de

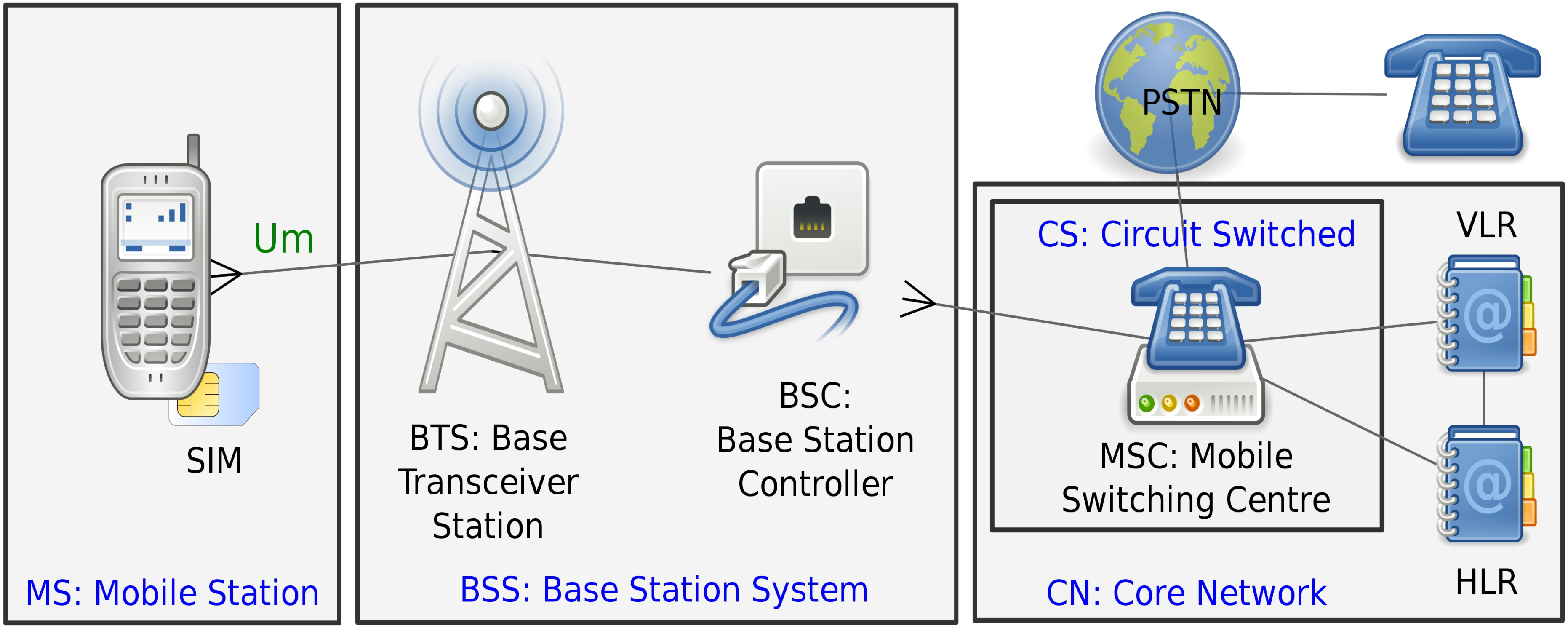
Agenda

- GSM architecture introduction
- Introduction to mobile paging
- Attacking paging
- Attacking large areas
- Conclusions

GSM wut?! protocol necrophilia?

- GSM has been beaten almost to death ;)
- Still one of the most relevant mobile telephony standards!
- Problems may affect other protocols: 3G, LTE, ...
- It's fun to play with radio!

GSM network infrastructure (simplified)



Introduction to paging

- Paging Channel (PCH) broadcast downlink channel on the CCCH
- PCH used by network for service notification

- Paging message carries Mobile Identity (TMSI/IMSI)
- Each phone compares its identity and reacts

- Again, this information is broadcast!

- Can we abuse this knowledge? ;D

CC by 2.0 Denis Apel

Mobile Terminated (MT) service delivery

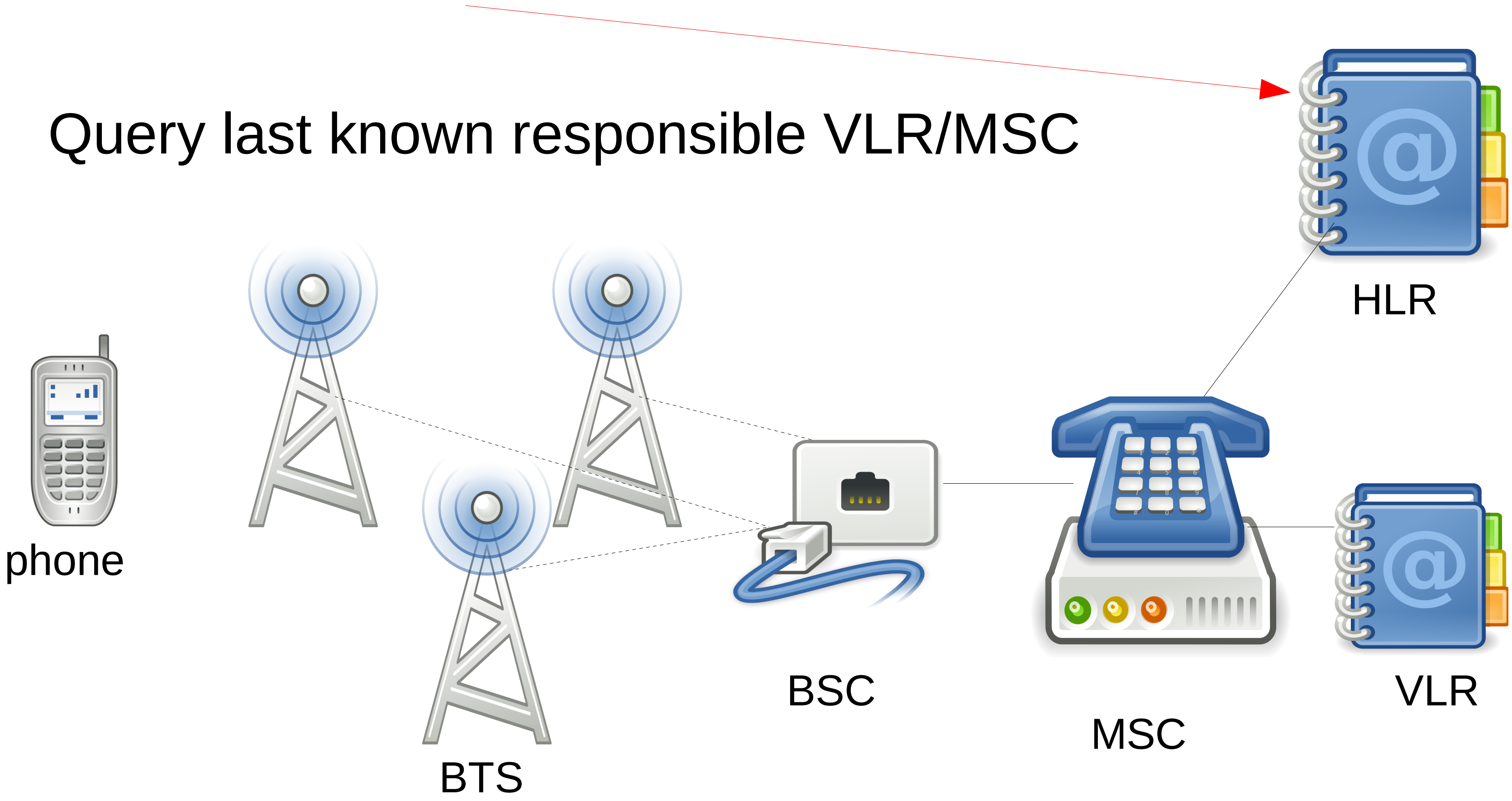
- Mobile phones idle most of the time
  → not in constant contact with the network
  → saves battery

- So which BTS should transmit the signal?
- Mobile networks needs to determine the phone's location

- Visitor Location Register (VLR) handles subscribers that are within a specific geographical area

Mobile Terminated service delivery cont.

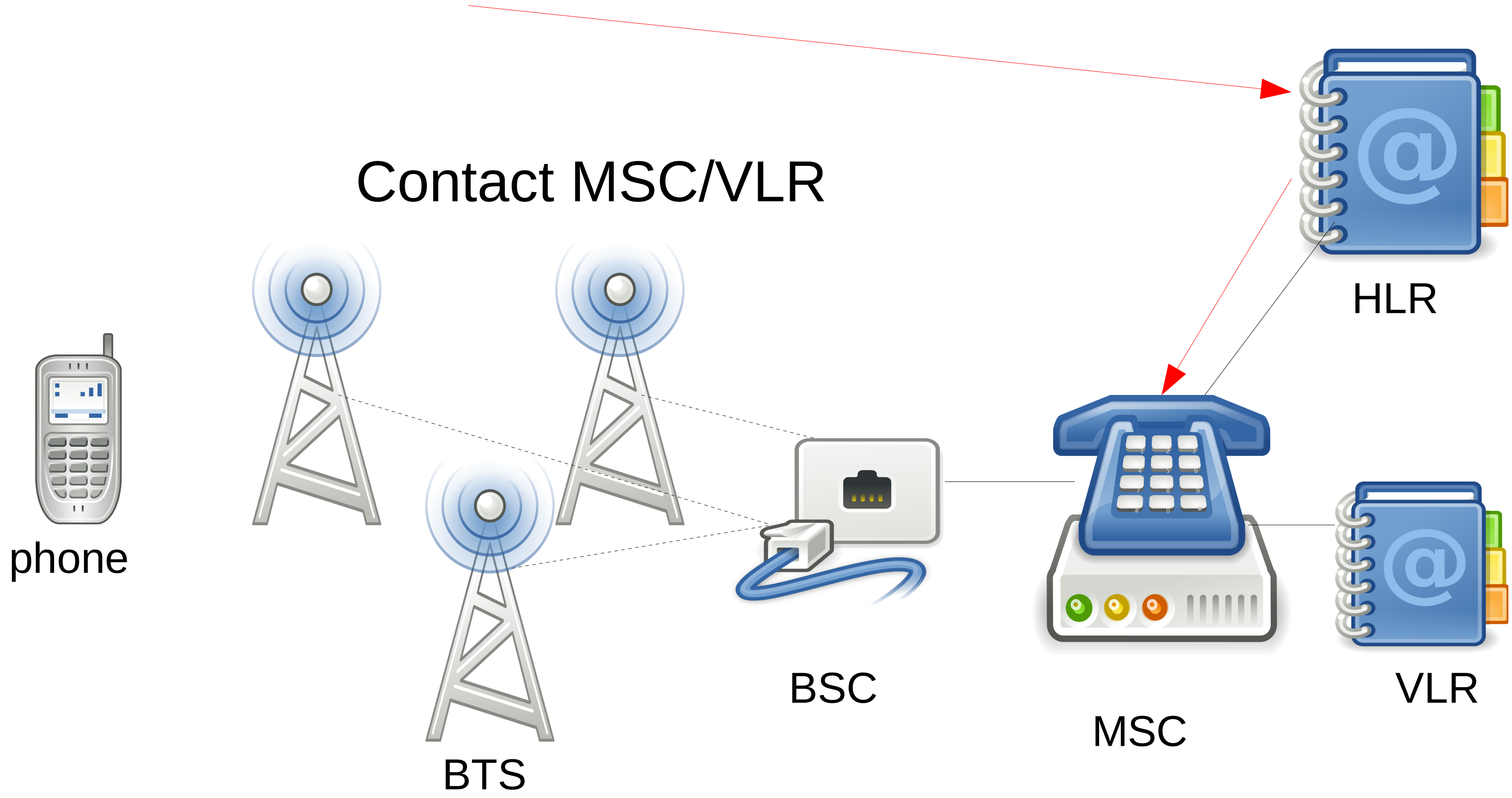
- What happens when you call or text someone?



Query last known responsible VLR/MSC

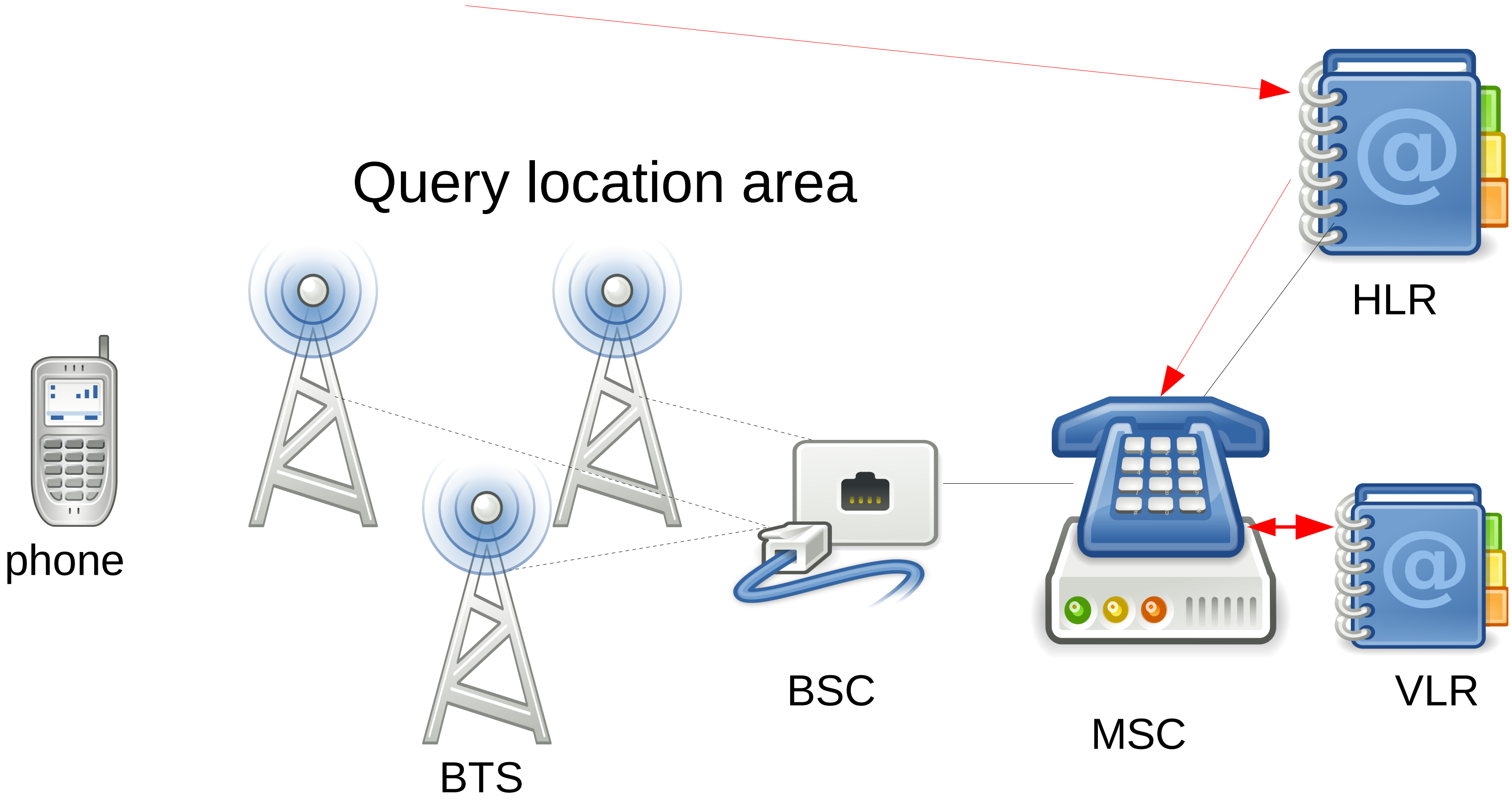
Mobile Terminated service delivery cont.

- What happens when you call or text someone?



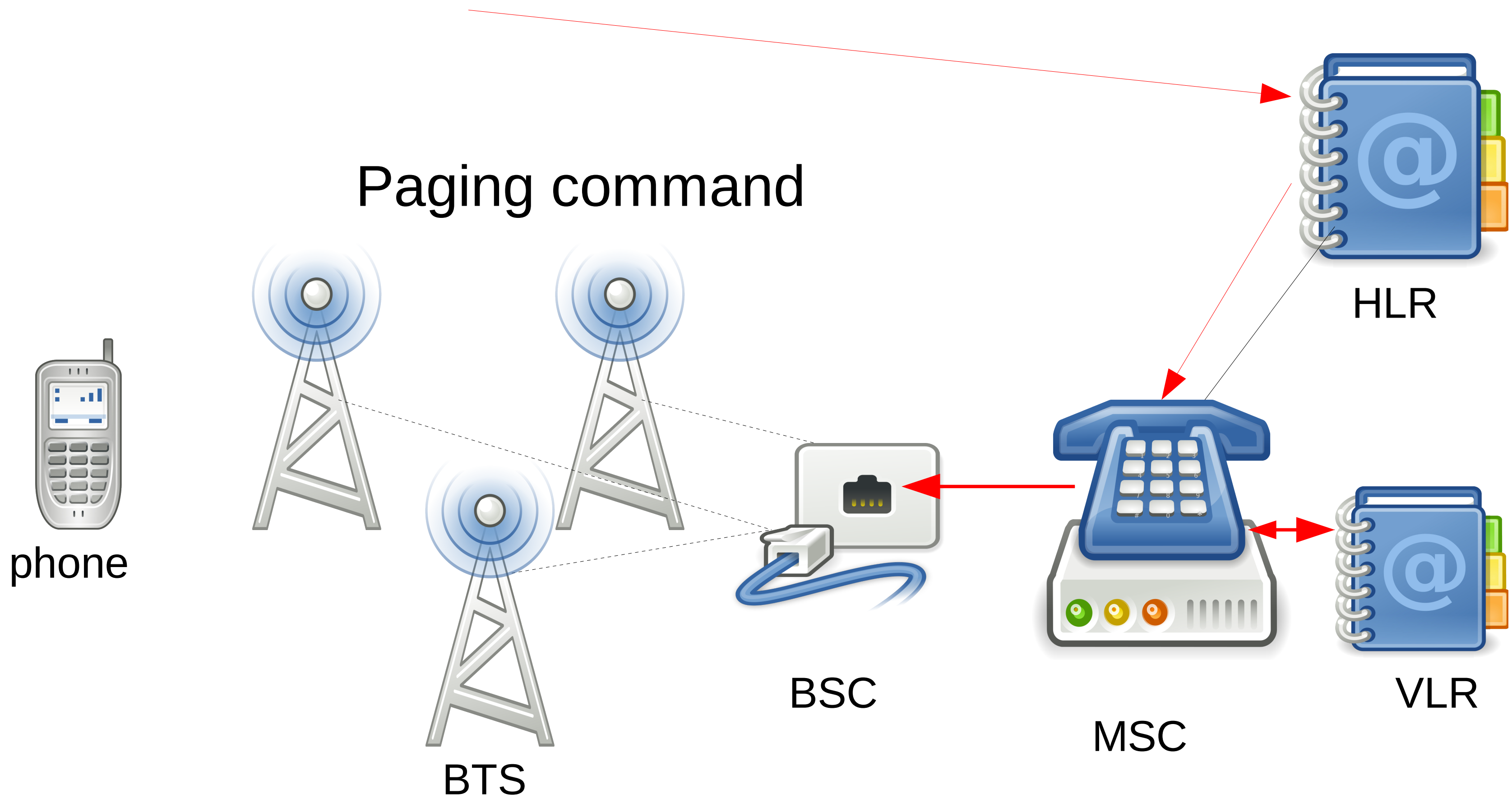
Mobile Terminated service delivery cont.

- What happens when you call or text someone?



Mobile Terminated service delivery cont.

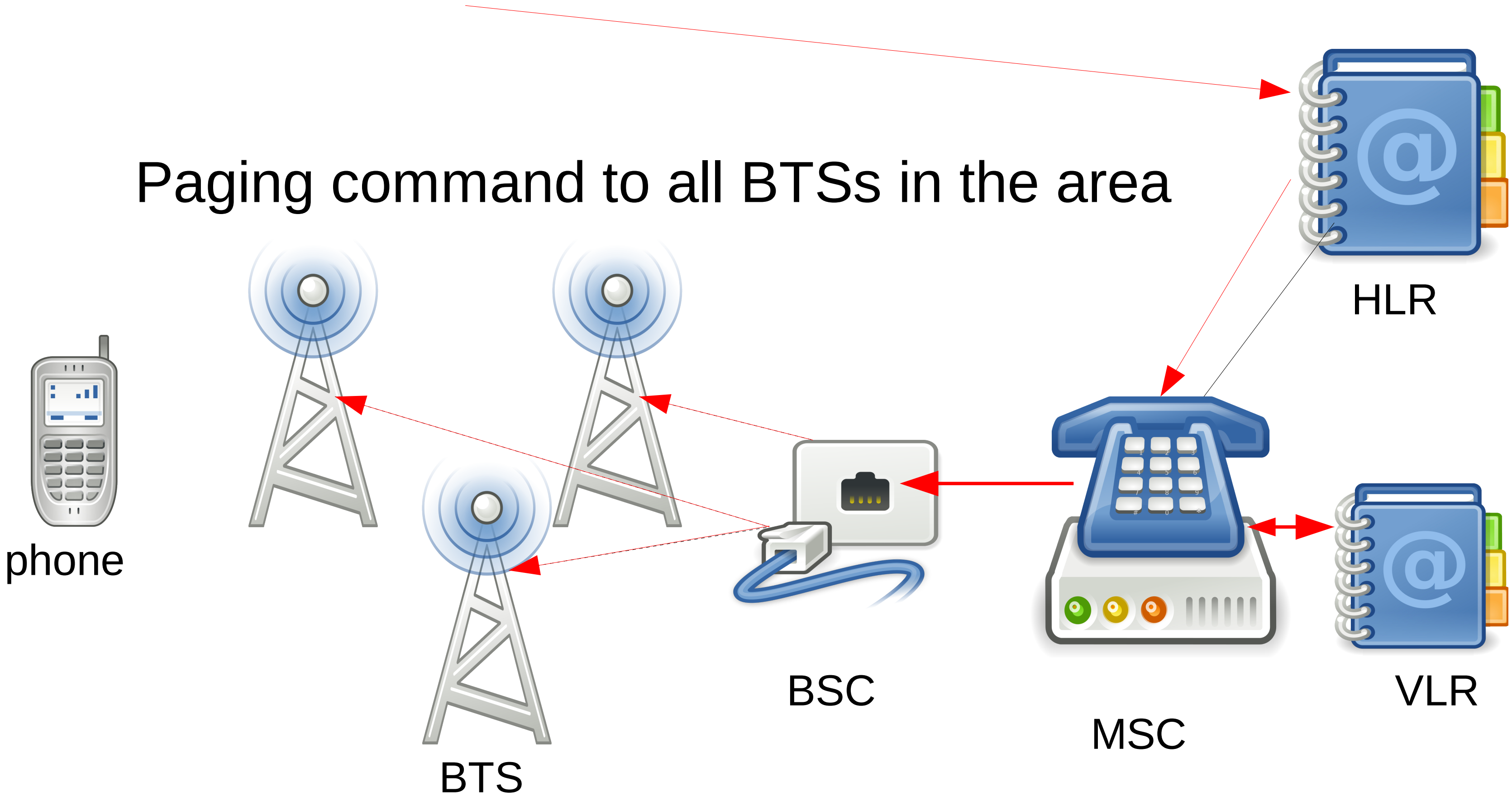
- What happens when you call or text someone?



Mobile Terminated service delivery cont.

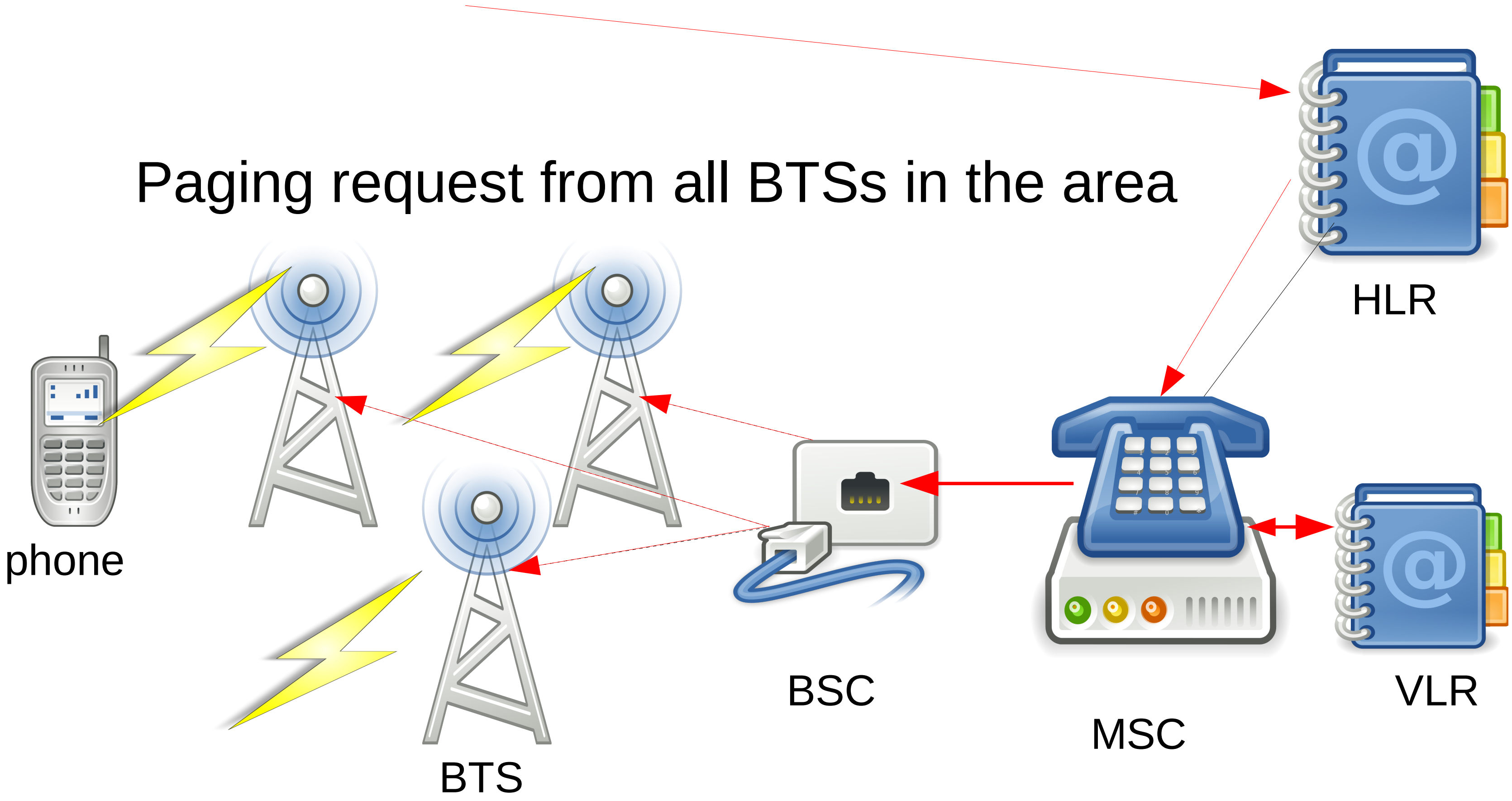
- What happens when you call or text someone?

Paging command to all BTSs in the area

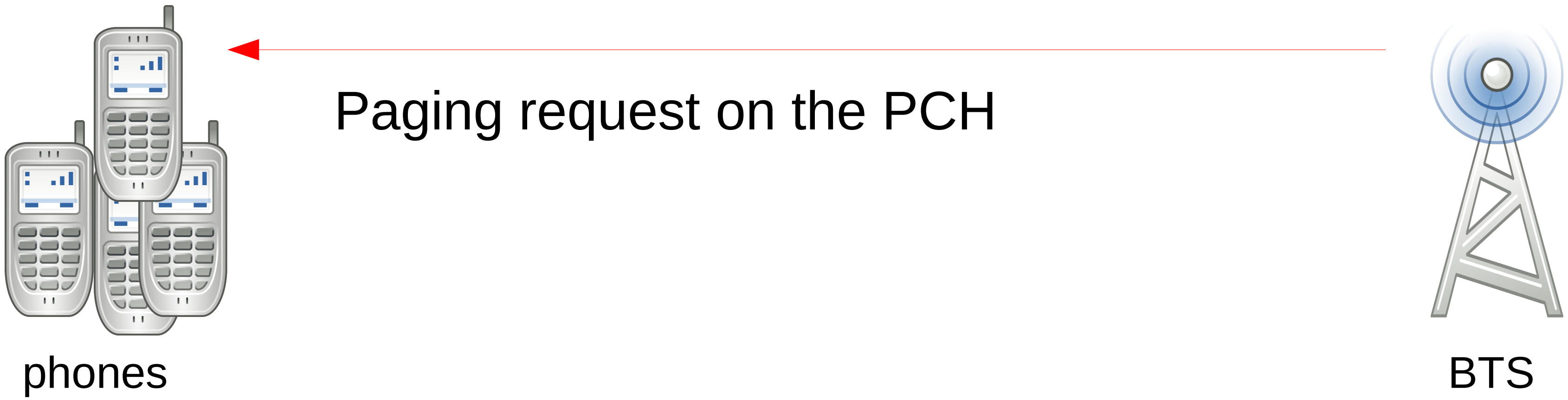


Mobile Terminated service delivery cont.

- What happens when you call or text someone?



Mobile Terminated service delivery cont.

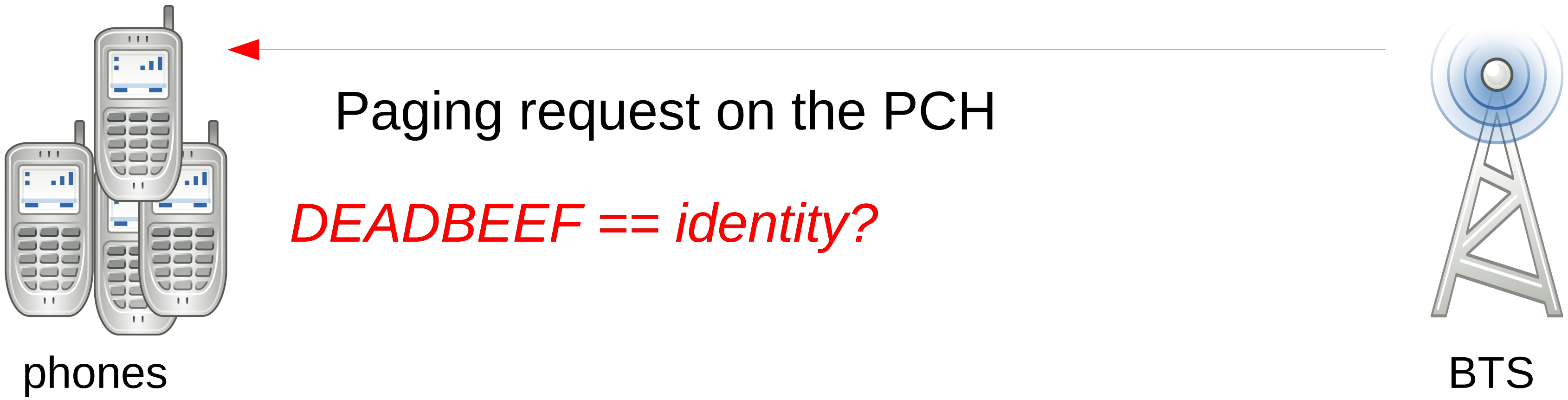


Paging request on the PCH

phones

BTS

Mobile Terminated service delivery cont.



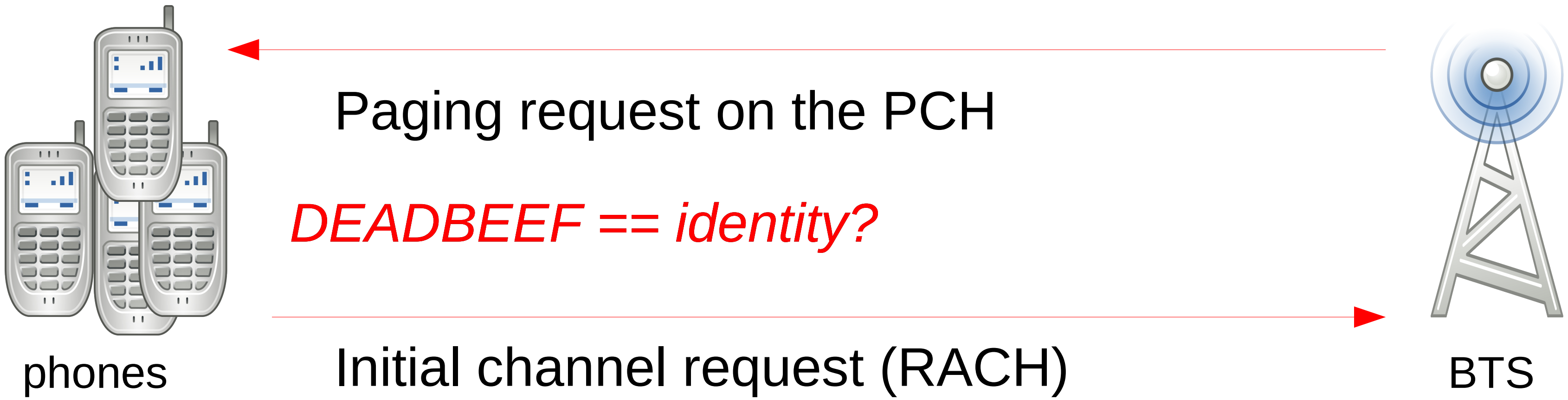
Paging request on the PCH

DEADBEEF == identity?

phones

BTS

Mobile Terminated service delivery cont.



Paging request on the PCH

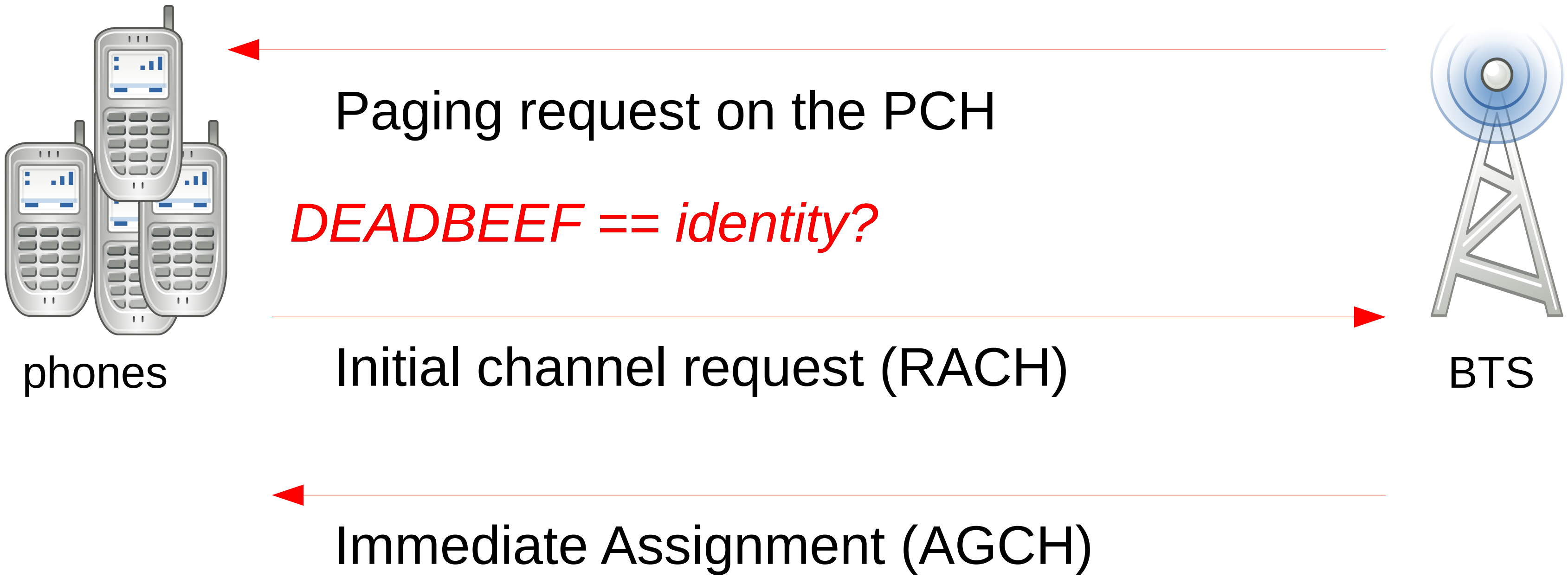
DEADBEEF == identity?

Initial channel request (RACH)

phones

BTS

Mobile Terminated service delivery cont.



phones

BTS

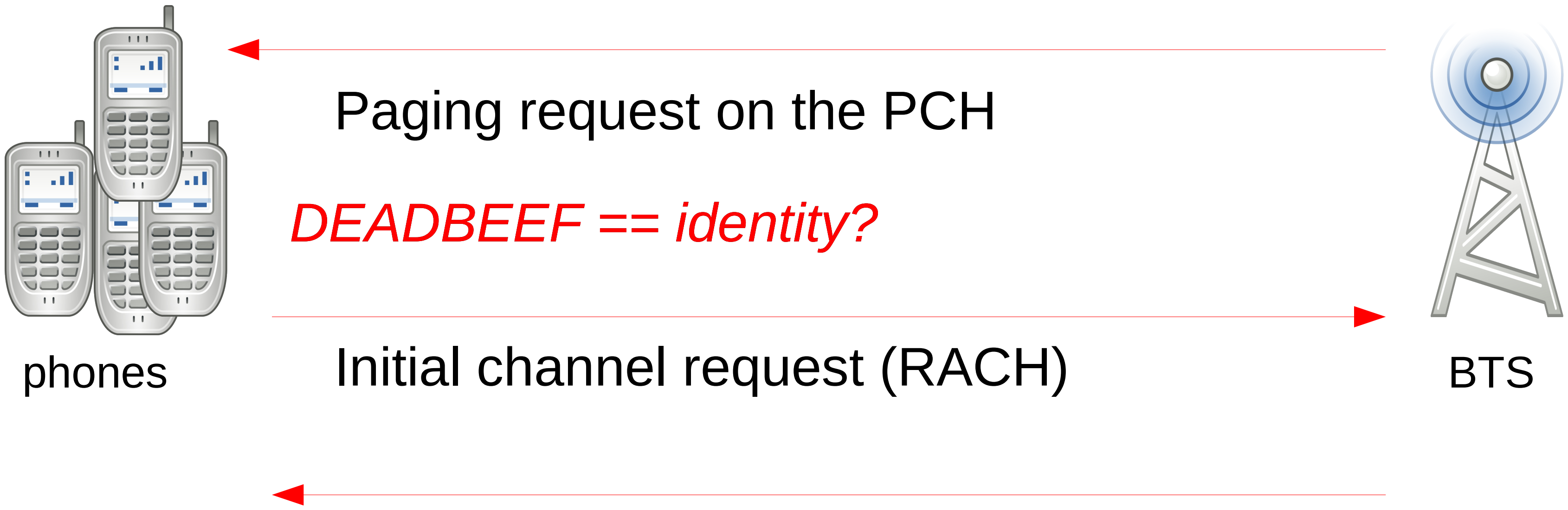
Paging request on the PCH

DEADBEEF == identity?

Initial channel request (RACH)

Immediate Assignment (AGCH)

Mobile Terminated service delivery cont.



phones

BTS

Paging request on the PCH

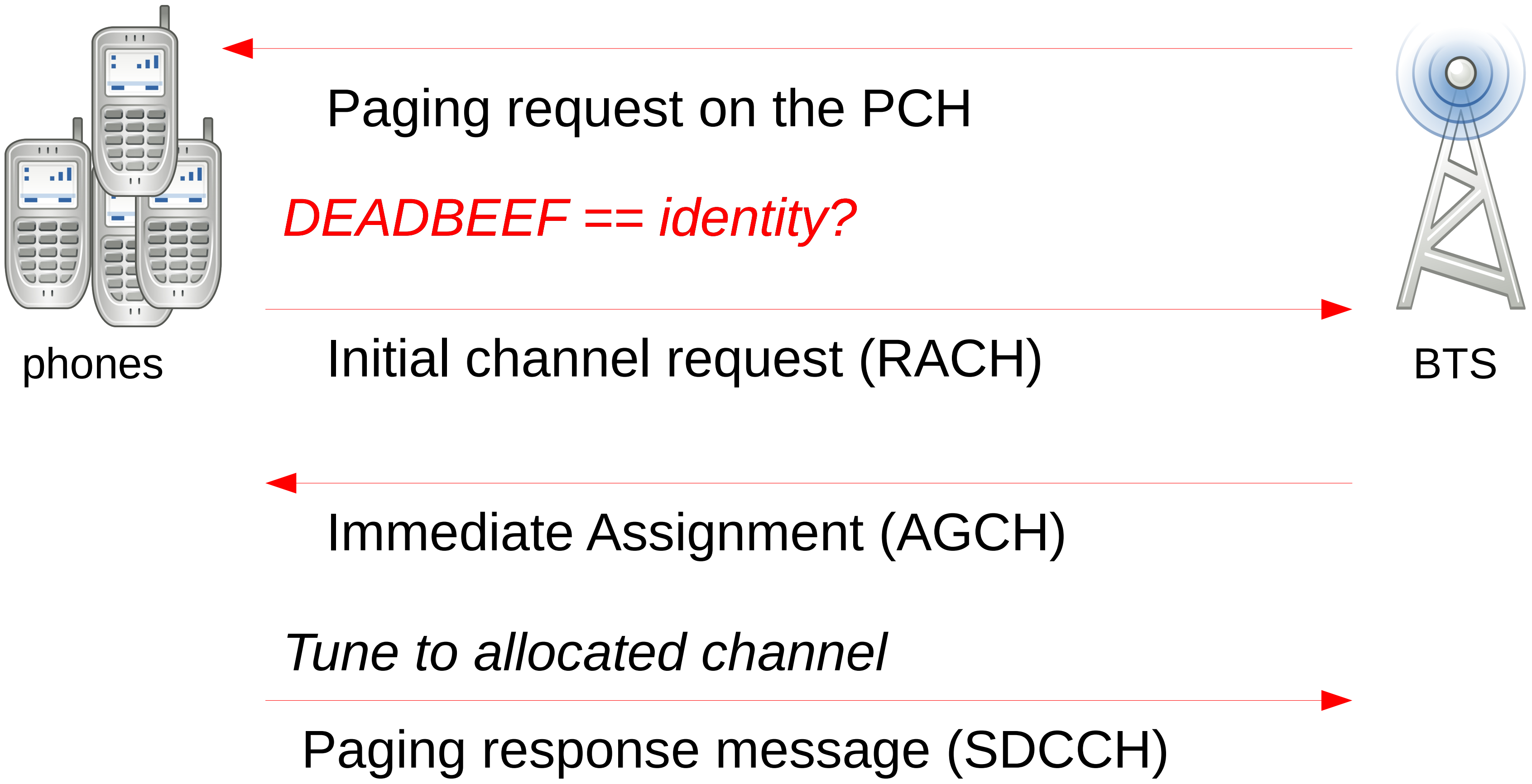
DEADBEEF == identity?

Initial channel request (RACH)

Immediate Assignment (AGCH)

Tune to allocated channel

Mobile Terminated service delivery cont.



phones

BTS

Paging request on the PCH

DEADBEEF == identity?

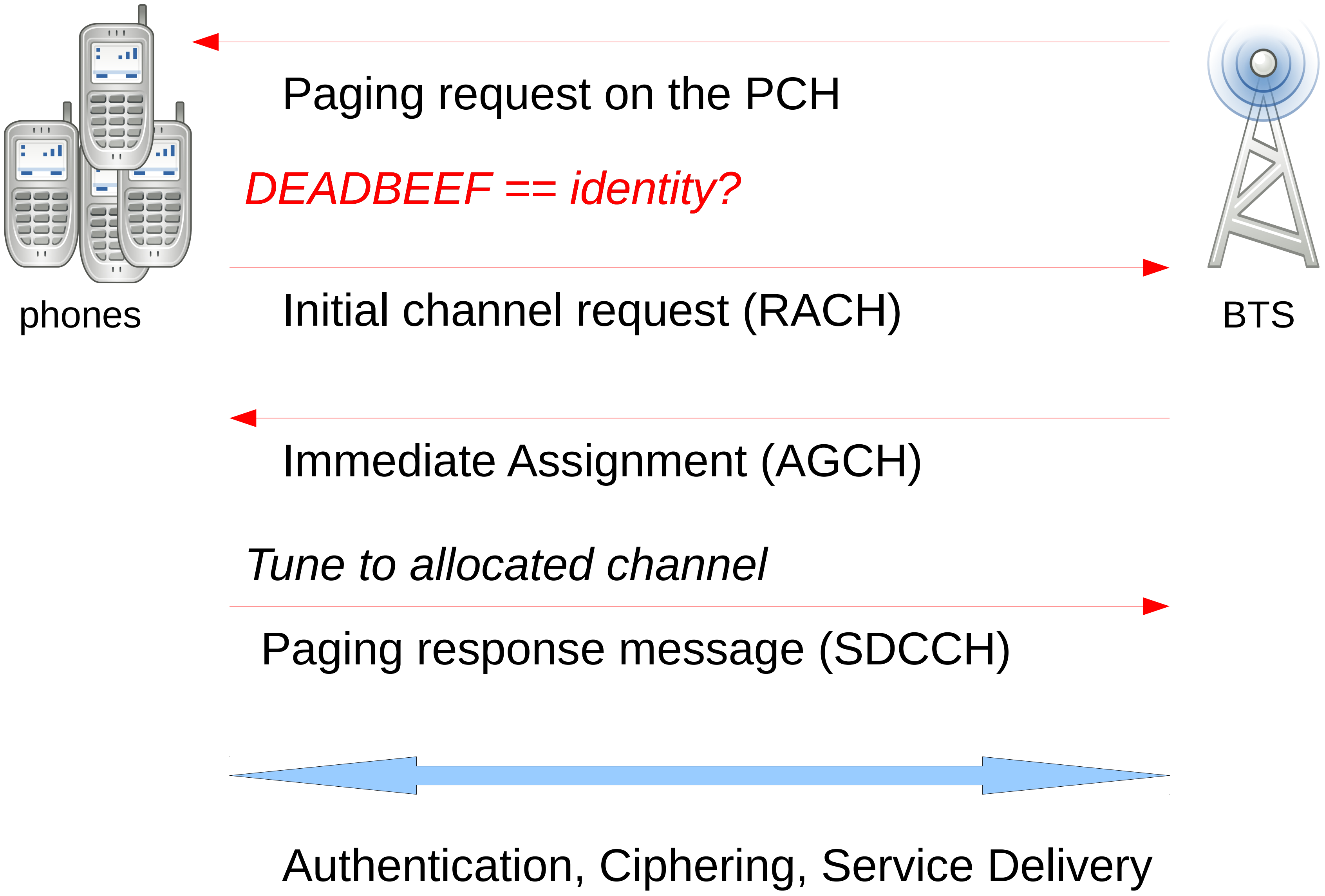
Initial channel request (RACH)

Immediate Assignment (AGCH)

Tune to allocated channel

Paging response message (SDCCH)

Mobile Terminated service delivery cont.



phones

BTS

Paging request on the PCH

DEADBEEF == identity?

Initial channel request (RACH)

Immediate Assignment (AGCH)

Tune to allocated channel

Paging response message (SDCCH)

Authentication, Ciphering, Service Delivery

Hijacking the service?

- Evil hackers can't just impersonate subscribers here
  - Well more on that later...
- Authentication and cipher information stored on the SIM card
- But what happens if we respond with wrong information or not at all?

→ channels are dropped, no service delivered (call, SMS) :(

Paging Attack

- We have a race condition!

- GSM protocols are driven by complex state machines
- State changes after:
  - Receiving paging response
  - Channel dropping

- Can we respond to other peoples paging messages?
- Can we do that faster?
- Will the network expect a 2nd paging response?

- We could do that from any BTS in the same area!

Paging Attack - What exactly is fast?

- Speed influences by many things
  - Weather
  - Radio signal quality
  - Network saturation
  - ....

- But mostly the **baseband** implementation!
  - Layer{1,2,3} queuing and scheduling

Paging Attack – implementing a fast baseband

- Free Software/Open Source mobile baseband firmware: OsmocomBB
  - Runs on cheap hardware (e.g. cheap Motorola C123)
  - Mobile phone application exists (but runs on PC!)
    → not fast at all :/
- Completely implemented as Layer1 firmware
  - Ported Layer2/Layer3 to Layer1
  - Runs solely on the phone → very fast
- Listens to messages on the PCH
- Can react to IMSIs/TMSIs or TMSI ranges
- Sends paging response messages
- Performs invalid ciphering/auth

Paging Attack - Measuring paging response speed

- Relevant baseband stacks:

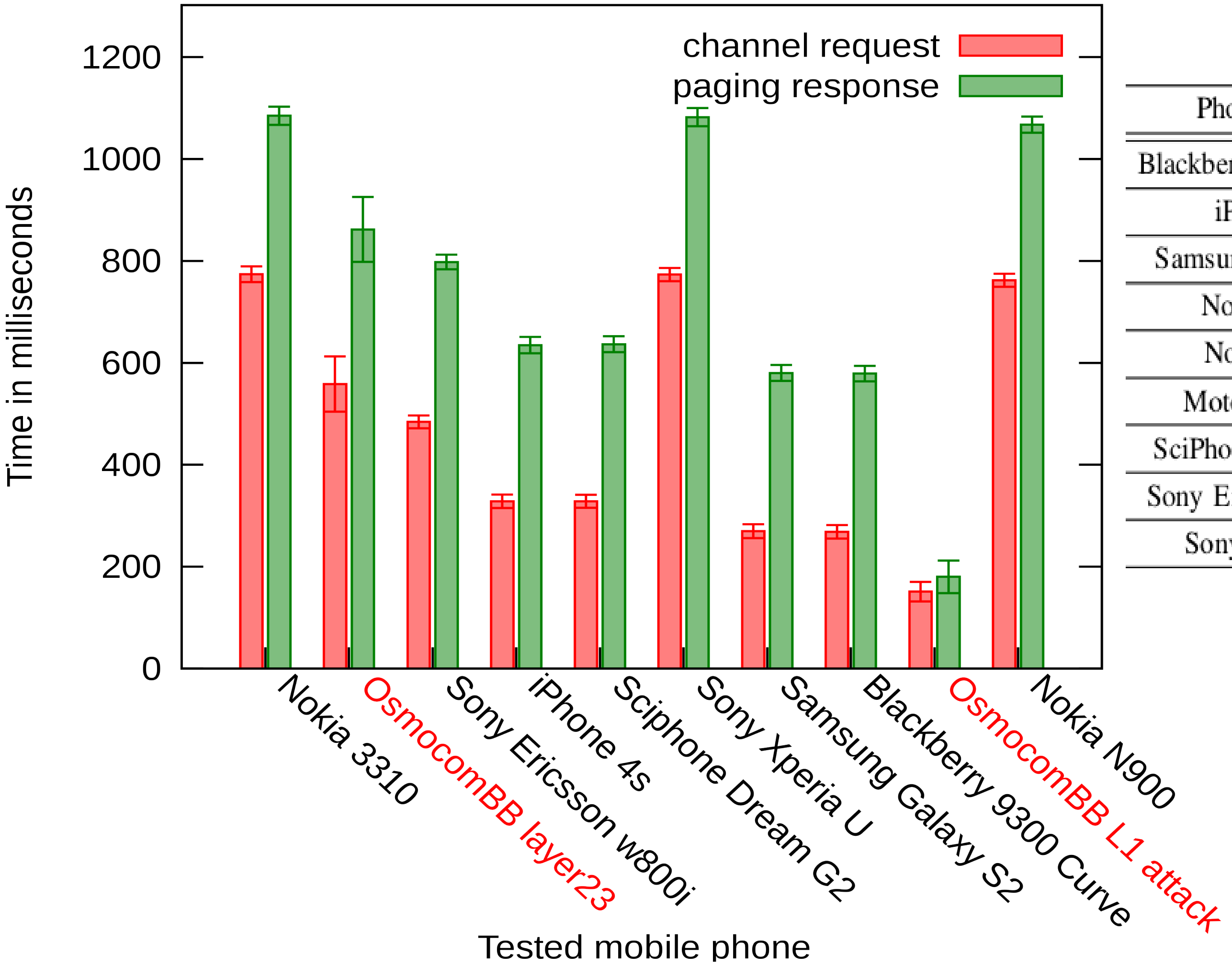
  Qualcomm, Intel (Infineon), Texas Instruments, ST-Ericsson, Renesas (Nokia), Marvell, Mediatek

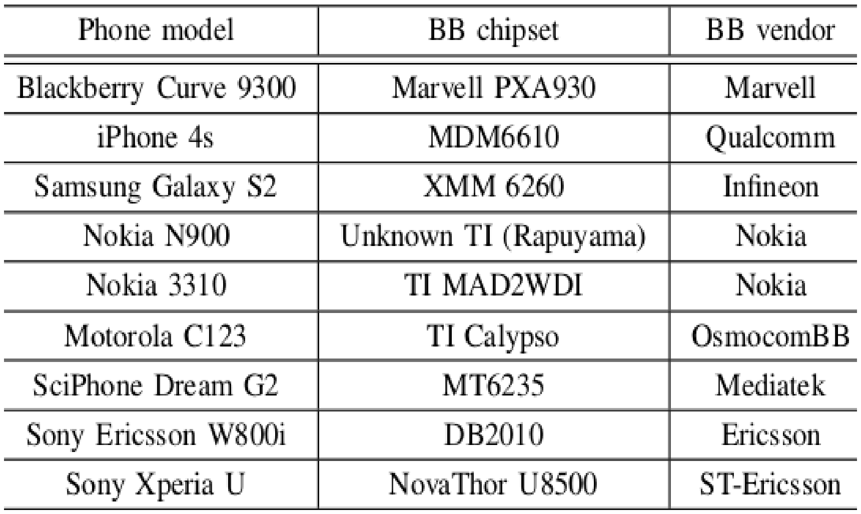
- USRP + Modified OpenBTS version logs:
  - Time for Paging Request ↔ Channel request
  - Time for Paging Request ↔ Paging response

- Hookup phones to test BTS
- Send 200 SMS to each phone
- Measure

Paging Attack - How fast is the “average” phone?

- Time measurements for each baseband





Phone model	BB chipset	BB vendor
Blackberry Curve 9300	Marvell PXA930	Marvell
iPhone 4s	MDM6610	Qualcomm
Samsung Galaxy S2	XMM 6260	Infineon
Nokia N900	Unknown TI (Rapuyama)	Nokia
Nokia 3310	TI MAD2WDI	Nokia
Motorola C123	TI Calypso	OsmocomBB
SciPhone Dream G2	MT6235	Mediatek
Sony Ericsson W800i	DB2010	Ericsson
Sony Xperia U	NovaThor U8500	ST-Ericsson

Paging Attack - Practice results

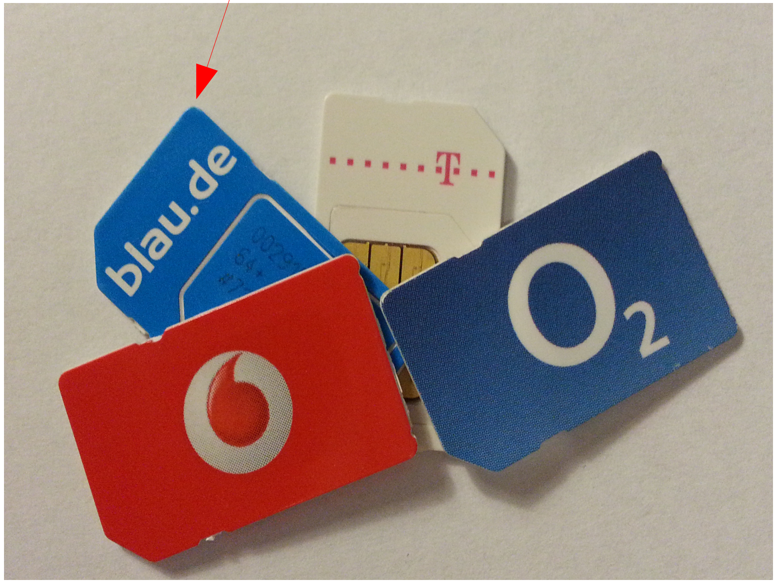
- OsmocomBB layer23 (modified mobile application) is too slow
- Small layer1 only implementation can win the race!

  → DoS against Mobile Terminated services

- Tested all German operators:
  - Vodafone
  - O2 (Telefonica)
  - E-Plus
  - T-Mobile

  → all vulnerable to this attack

E-Plus MVNO



DEMO – DoS

Getting victim mobile identities

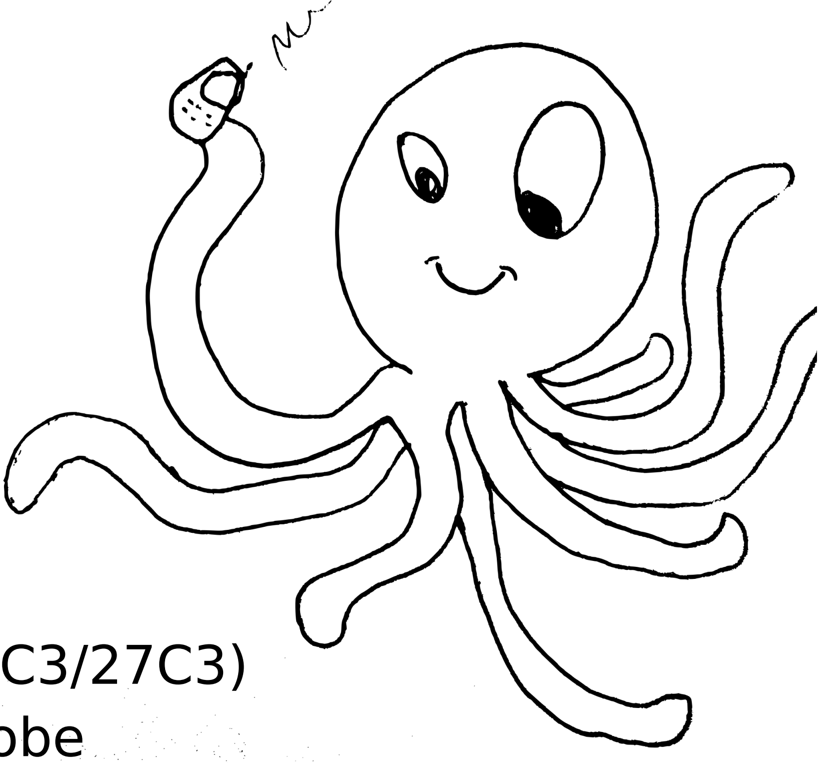
- You don't necessarily have to (why not just react to every paging?)
- Network paging with IMSIs:
  - 3rd party HLR lookups provide number → IMSI mapping
- For TMSIs:
  - Monitor PCH with OsmocomBB phone
  - Call victim, drop call early (3.7 seconds on O2)

    → phone will not ring, but being paged!
  - Or use silent SMS
  - Rinse and repeat

→ Evaluate monitored data

“Location leaks over the GSM air interface”, Kune et al., NDSS 2012
“Wideband GSM Sniffing”, Munaut & Nohl, 2010

Hijacking delivery – Encryption



- We need Kc for encrypted communication!

- Some networks use A5/0 → No encryption
- Some networks use A5/2 → Broken (1999)
- Most use A5/1 → Broken (e.g. 26C3/27C3)
  - Kraken + OsmocomBB phones/airprobe can crack session key (Kc) in seconds

- Not many A5/3 networks due to phone implementations

Paging Attack cont. – Authentication

- 50% of networks authenticate MT (SMS/call) 10% of the time
  (referring to Security Research Labs)

- Operators care about MO because of billing!
- However, MT indirectly affects billing

- Most MT service deliveries not authenticated

© Julien Tromeur

- Incomplete authentication allows MT hijacking
  → Our code can handle a known session key/encryption

DEMO – Hijacking SMS

Broken Authentication - O2

- When receiving authentication request, attacker does not respond
- When victim does, attacker channel also authenticated
  → next step is ciphering

- Network seems to only know about authenticated subscriber
  - Not authenticated channel!

- Phone's can easily be forced to authenticate by causing paging ;)

- For those interested:
  http://pastie.org/private/jbp1yji4f0i2ara2awkq

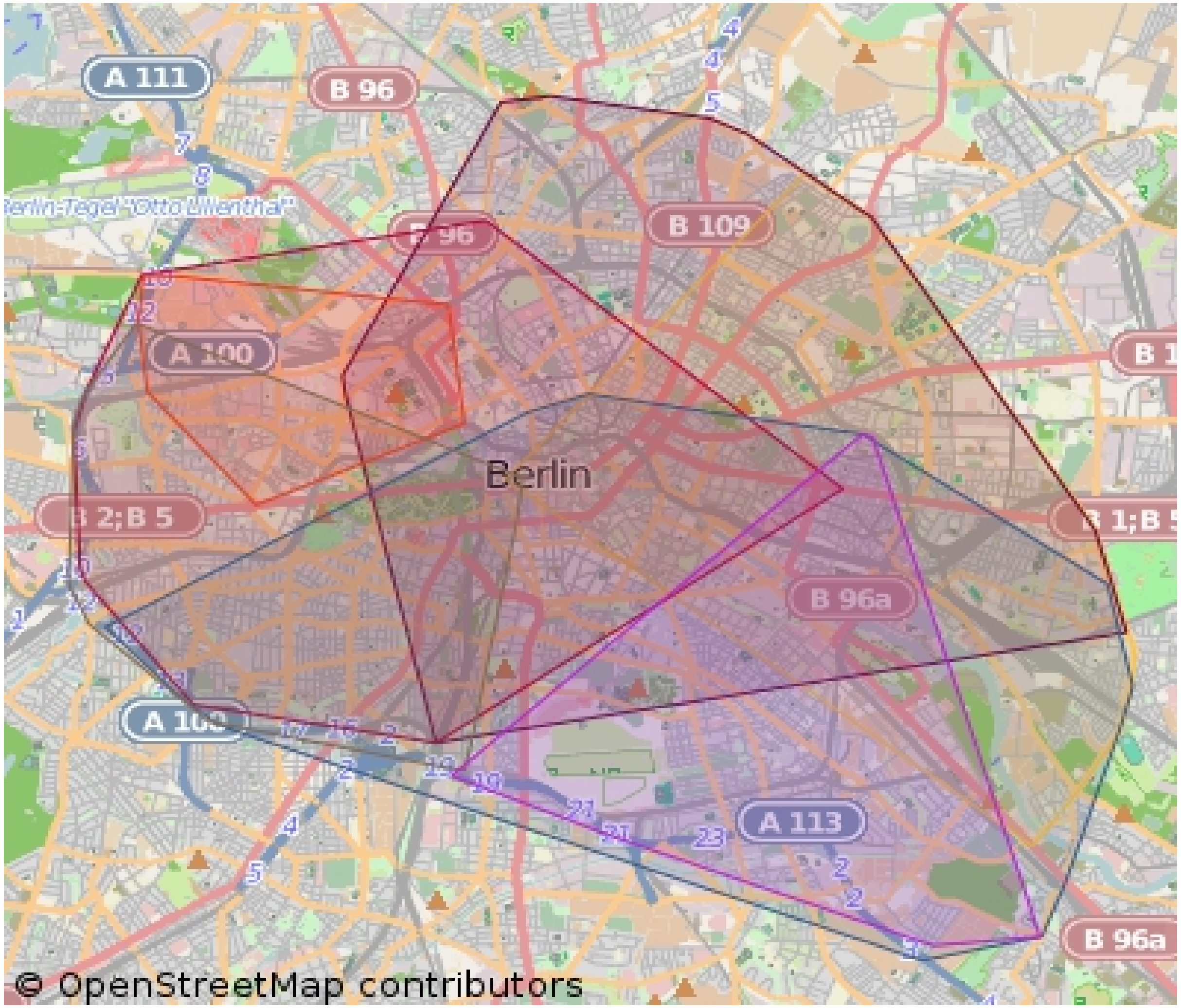
Attacking large areas

- VLRs handle larger geographical areas (Location Area)
- Paging broadcasted on all BTSs for that area
  → we don't need to camp on the same BTS
- Respond to all paging requests faster for Location Area
  → DoS to all subscribers in that area

How large is a Location Area?

- Location Area Code broadcast on the BCCH
- 2 people + GPS loggers + OsmocomBB cell_log phones + car :)

Location Areas – Berlin/Vodafone

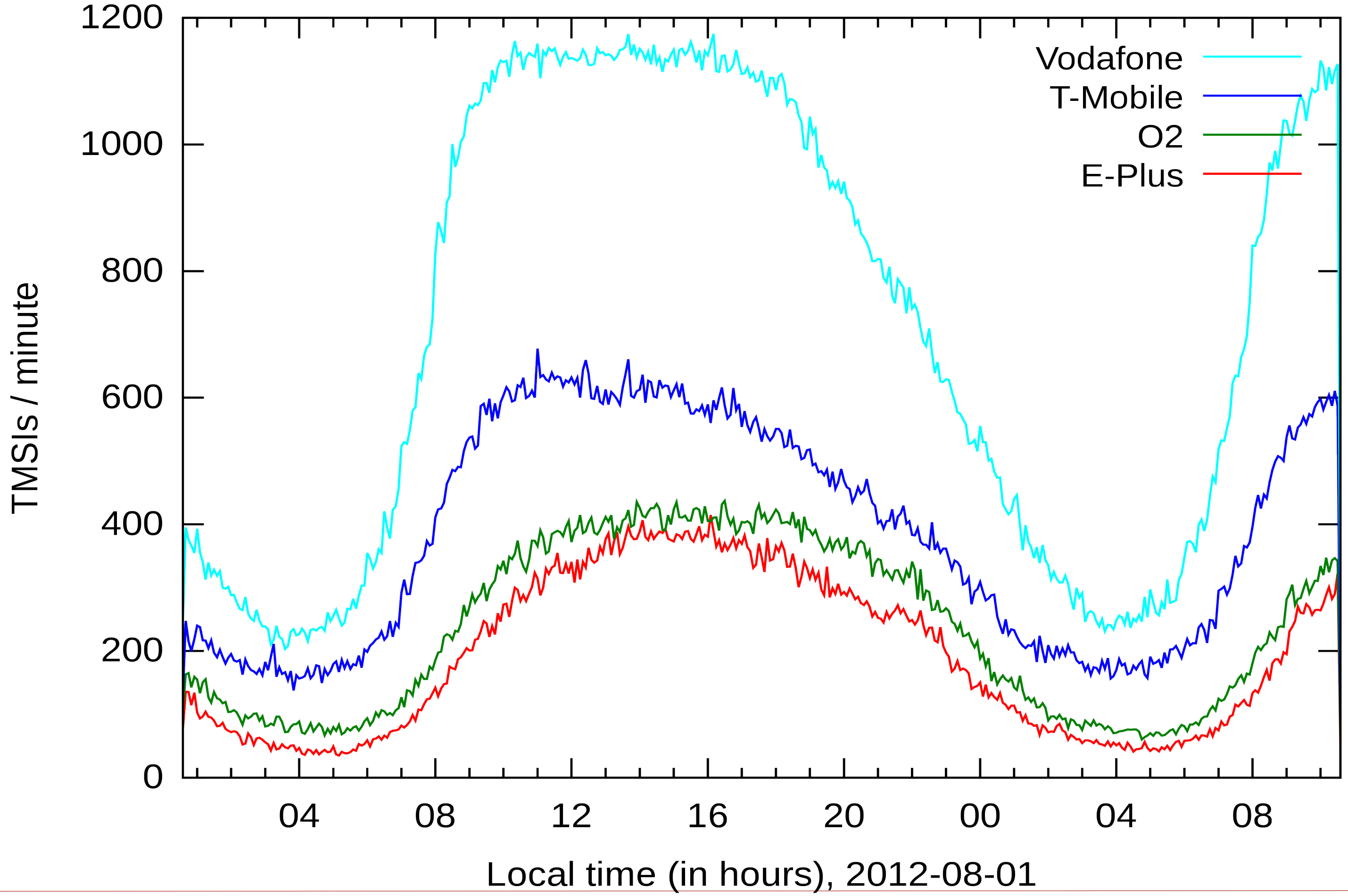


Attacking Location Areas cont.

- Non-city LAs larger (and fewer) than for cities
  - Seen 1000 km^2
- Location Areas are huge even in cities!
  - 100 – 500 km^2 in Berlin
  - Cover whole city districts
- For Mobile Terminated:
  Paging DoS way more effective than jamming
- Feasibility depends on paging activity

Attacking Location Areas - Activity

- We can camp on location areas and log paging
- Measured all 4 operators over 24 hours, same time and location



DoS + Paging activity reduction

- Paging attack stops initial service delivery
- We don't want to answer every time in the future

- IMSI DETACH attack by Sylvain Munaut
- Phone detach signal to network
  → Mobile Terminated services not delivered until re-attach

- Detach message contains mobile identity
  → send paging response, send detach message
  → watch paging reducing over time

Attacking Location Areas cont.

- For a small operator (E-Plus) 415 TMSIs in paging / minute
- Vodafone even 1200! (But paging twice)

- We are not that fast!
  - Resynchronization takes time

- Paging response is on a dedicated channel
  - PCH not visible during attack

→ Definitely not feasible with one phone

Attacking Location Areas cont.

- These phones are cheap though (5-20 €)

Conclusions

- Attacking single subscribers and Location Areas is practical!

- MT services need 100% authentication
- Active attackers (malicious phones) need to be considered by standardization bodies

Thank you for your attention!

- Also thanks to these people:
  - Dmitry Nedospasov
  - Dieter Spaar
  - Holger Freyther
  - Harald Welte
  - Tobias Engel
  - Osmocom community!

- Disclaimer:
  - Don't do this at home...

    … or only with your own SIM cards!

Questions?

- Source code will be published, stay tuned
  check http://nion.modprobe.de/blog/ after new year.

- Poke me if I forget
  - nico@sec.t-labs.tu-berlin.de
  - @iamnion