Mobile Information Systems

Lecture 02:
Location & Networks

© 2015-25 Dr. Florian Echtler
Bauhaus-Universität Weimar
Aalborg University

Networks: Overview

- Basics (continued)
  - Multiplexing, multiple access methods
- Examples
  - Bluetooth (WPAN)
  - 802.11x WiFi (WLAN)
  - GSM/UMTS/LTE (WWAN)

Networks: multiplexing

- RF spectrum is a precious shared resource
  (see US frequency allocation chart)
- Allocated band has to be shared among many different transmitters without interference
  → requires *multiple access method*

Networks: multiple access (1)

- Time-division multiple access (TDMA)
  - Static: “timeslots”
    - One single transmitter active per slot
    - Requires clock synchronization in advance
  - Dynamic: carrier-sense multiple access/collision avoidance (CSMA/CA)
    - Listen if channel idle, then transmit (carrier sense)
    - (Optional) Request to send/clear to send (RTS/CTS)
→ “hidden node problem” (X ↔ Ap ↔ Y)
    - Transmit and wait for acknowledgement (collision detection during transmission almost impossible)

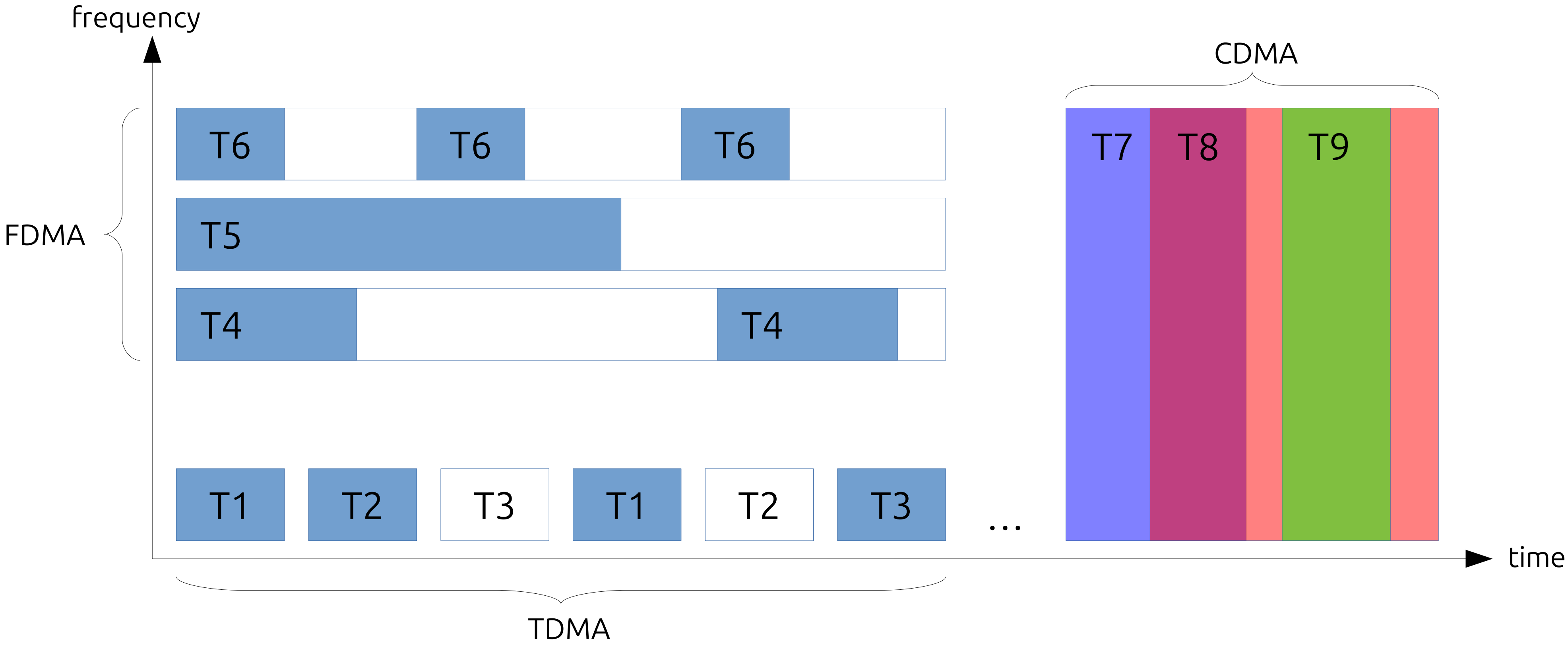
Networks: multiple access (2)

- Frequency-division multiple access (FDMA)
  - Simplest case: one frequency slot per transmission
    → receiver must be able to cover multiple slots
  - Complex variant: OFDMA (*orthogonal* …)
    - Simultaneous transmission of multiple low-bandwidth signals on "orthogonal" sub-channels
  - WDMA (*wavelength* …) → different light colours in optical transmission

Networks: multiple access (3)

- Code-division multiple access (CDMA)
  - Spread-spectrum method: uses wider spectrum than required for actual signal bandwidth
  - Multiple different modulation codes → allow separation of signals on same carrier
    - Frequency-hopping spread spectrum (FHSS)
      → code is pseudo-random sub-channel sequence
    - Direct-sequence spread spectrum (DSSS)
      → code is high-rate pseudo-random bit sequence

Networks: multiple access (4)

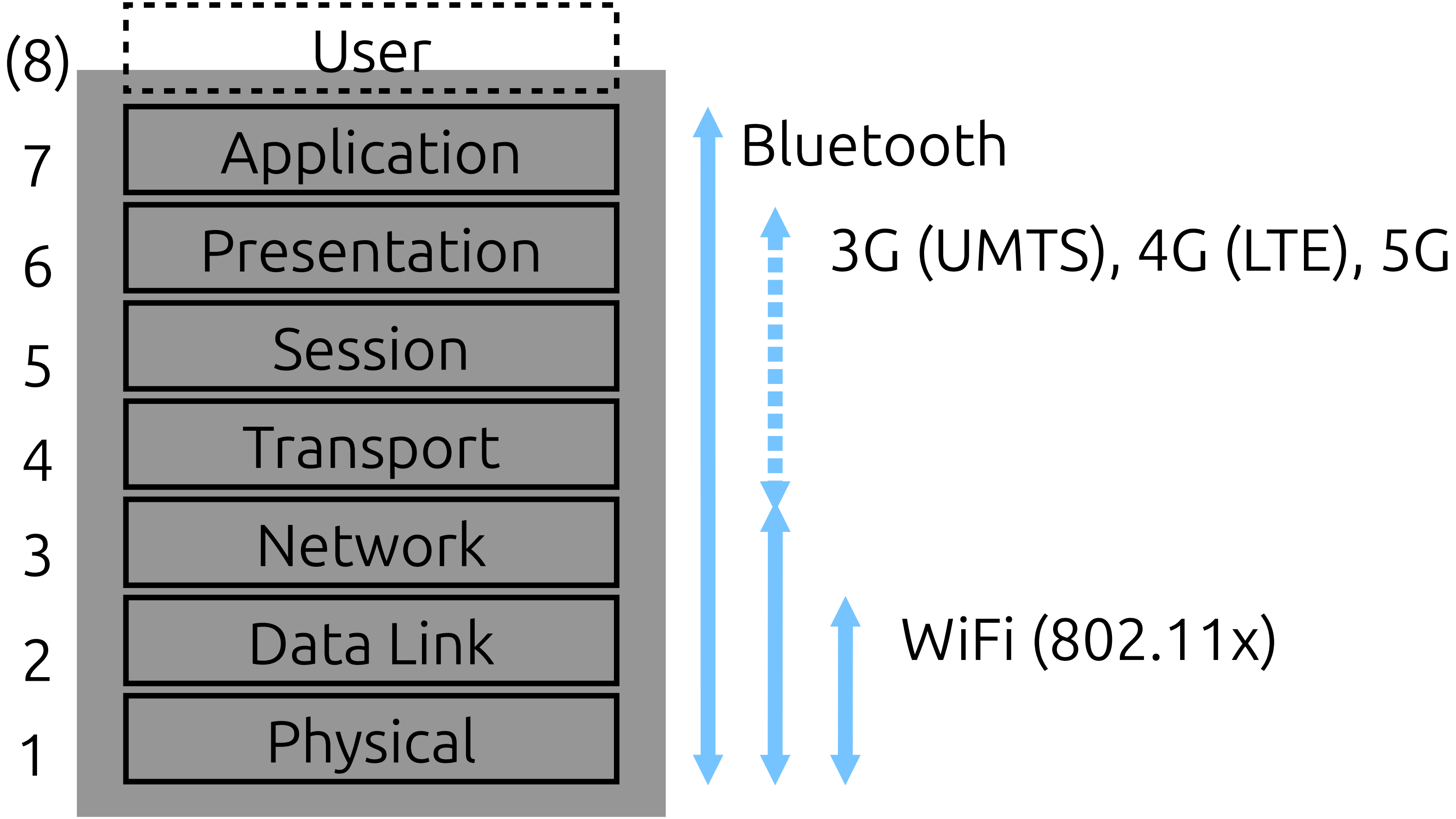


Assumption: transmitters T1 – T9, all using same signal bandwidth

Networks: summary

- Wireless networks need *multiple access method*
  - Timeslot-based: TDMA
  - Frequency-based: FDMA
  - Encoding-based: CDMA
- Mostly on lowest two levels of ISO/OSI model

Standards: ISO/OSI model



Standards: Bluetooth (1)

- Wireless *personal* area network (WPAN)
- Complex protocol stack across all layers
- Current specification (v5.2): 3256 pages (!)
- Air interface:
  - 2.4 GHz ISM band, up to 3 Mbit/s data rate
  - 80 channels á 1 MHz (or 40 * 2 MHz)
  - Adaptive frequency hopping (AFH), also known as frequency-hopping spread spectrum (FHSS)

Standards: Bluetooth(2)

- Two *incompatible* sub-specifications:
  - “Classic” Bluetooth
    - Used by headsets, mice, keyboards, …
  - Bluetooth Low Energy (BTLE/BLE), since v4.0
    - Used by sensors, wearables, …
    - Mesh support since v5.0
- Devices can support one or both standards
  - Most mobiles & laptops since ~ 2011 support both

Standards: WiFi™ (1)

- Wireless *local* area network
- Based on 802.11x standards family
- Also in 2.4 and 5 GHz ISM band
  - Interference with Bluetooth possible
  - Minimized with BT/WiFi integrated transceivers
  - WiFi can be used as high-speed data link layer for Bluetooth connections
- Data rates of up to ~ 10 GBit (in theory), in real-world scenarios up to ~ 1 GBit

Standards: Wi Fi™ (2)

- Only 2 lowest ISO/OSI layers
  - Physical layer: modulation & channel access
    - FHSS, DSSS or OFDM, depending on sub-standard, optionally + MIMO
  - Data link layer: management, e.g.
    - Announcement of SSID (Service Set ID = network name)
    - Roaming between access points
    - Encryption/authentication
- Many well-separated sub-standards
  → easier to implement than Bluetooth

Standards: WiFi (3)

- Network topology: usually star (or tree)
  - central access point(s), uplink via wired network
  - mobile devices connect to APs
  - roaming possible between APs in same network
- Alternative: WiFi Direct (or WiFi P2P)
  - local point-to-point network without AP
  - supports multiple devices (> 2)
  - often buggy, not well supported

Standards: WiFi™ vs. Bluetooth

Source (FU): http://www.ecnmag.com/article/2012/03/wi-fi-and-bluetooth-coexistence

- Same frequency band (2.4 GHz)
- Different modulation scheme (DSSS vs. FHSS)

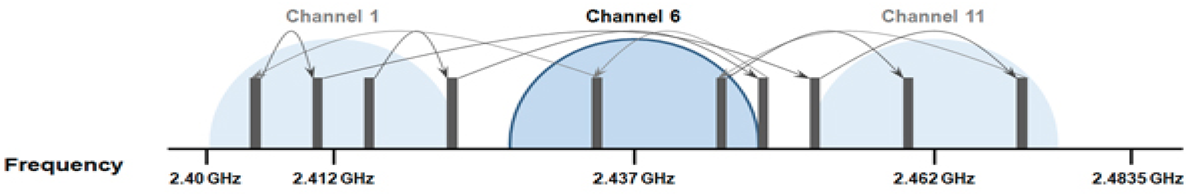


Figure 3. FHSS and DSSS transmissions will collide when the FHSS transmitted hops to a portion of the operating band occupied by the DSSS transmitter.

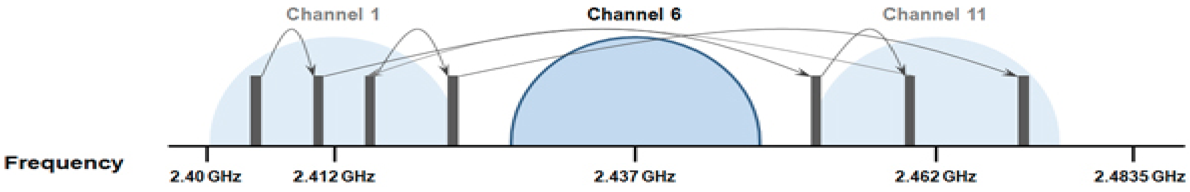


Figure 4. With AFH, FHSS devices avoid DSSS channels to allow for improved performance for both Bluetooth and Wi-Fi devices.

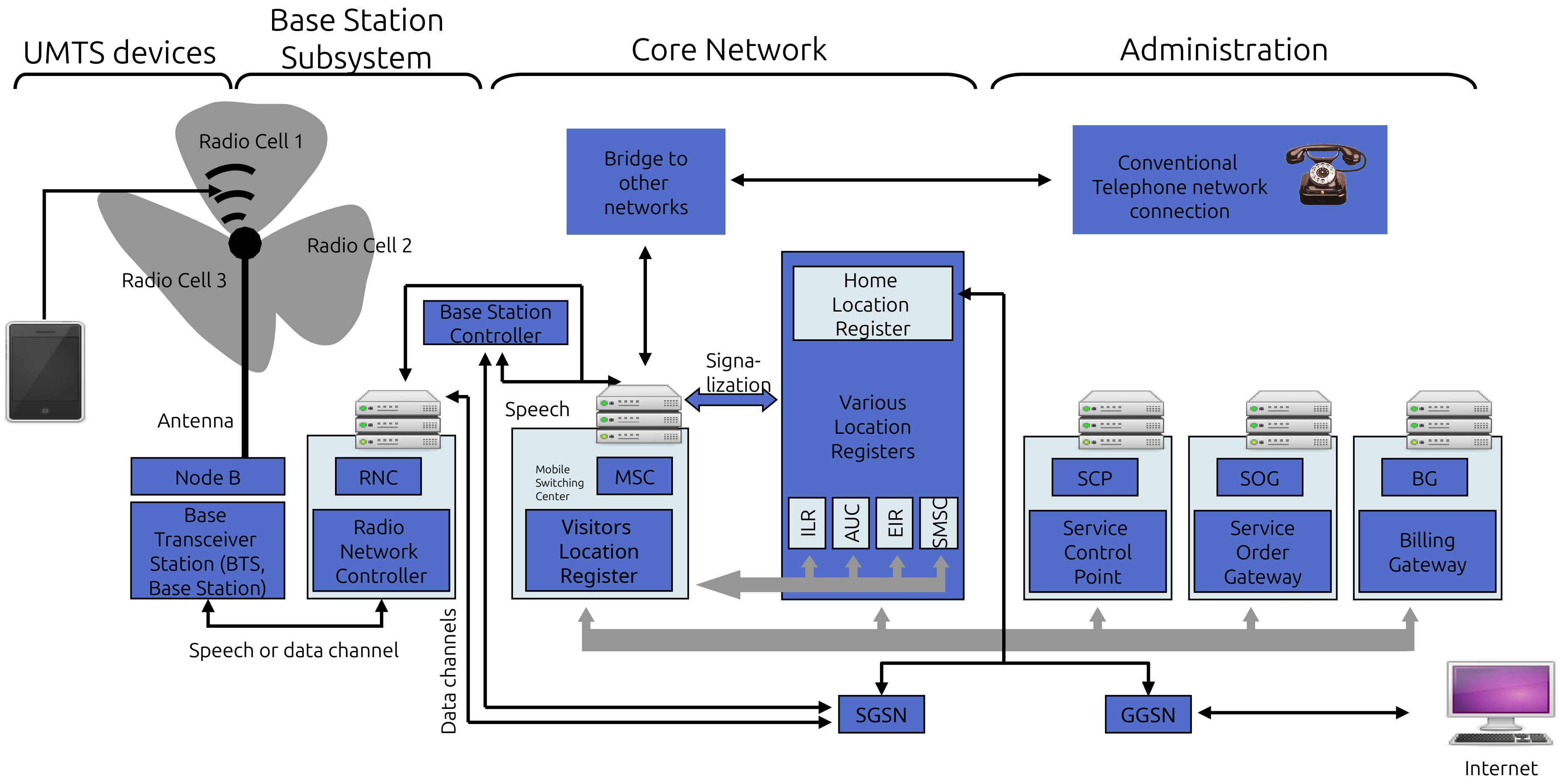
Standards: WWAN – 1,2,3,4,5G

- Wireless *wide* area networks history:
  - 1G – “C-Netz” (1985 – 2000): analog, FDMA, 9.6 kBit
  - 2G – GSM (1991 – now): digital, TDMA, ~ 200 kBit
    - 2015: phase-out beginning in some countries
  - 3G – UMTS (1998 – now): digital, CDMA, ~ 20 MBit
    - Hybrid circuit-switched and packet-switched network
  - 4G – LTE (2009 – now): digital, OFDMA, ~ 300 MBit
    - Purely IP-based, backend network less complex
  - 5G – (2020 - ?): digital, ~ 2 GBit, initial deployments
    - Support for IoT, campus networks, microcells, Car2Car, …

Standards: UMTS (3G)

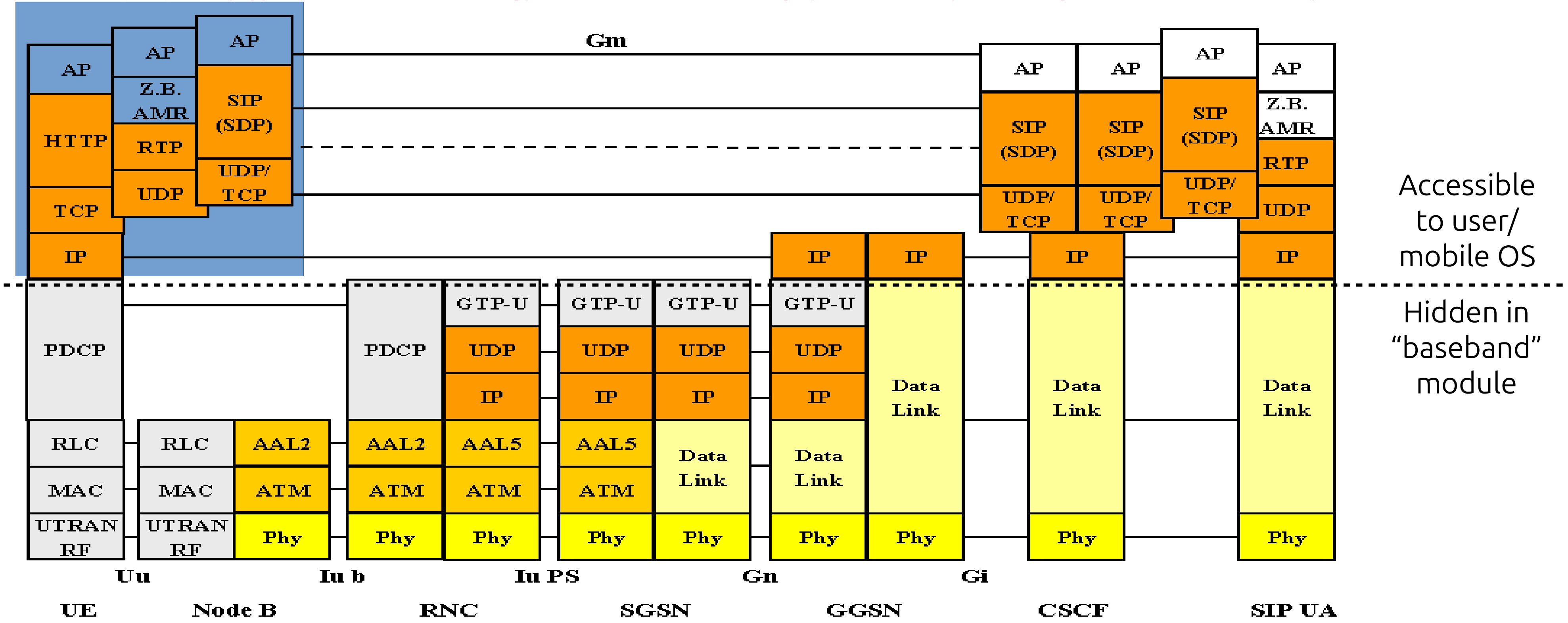
- Current de-facto WWAN standard
- Slowly being replaced by LTE
- Very complex hybrid between:
  - circuit-switched (~ old telephone network)
  - packet-switched (~ IP-based network)
- Most functionality/complexity hidden from user
  - Encapsulated in “baseband” module
  - Separate firmware/OS, processor, memory
  - Security/privacy issues? Nobody knows…

Standards: UMTS network schema



Standards: UMTS protocol stack

Source (FU): http://www.e-technik.org/aufsaetze_vortraege/aufsaetze/trick_itg_mobilfunk_6_03.pdf



RF = Radio Frequency
MAC = Medium Access Control
RLC = Radio Link Control
PDCP = Packet Data Convergence Protocol
GTP-U = GPRS Tunneling Protocol - User plane

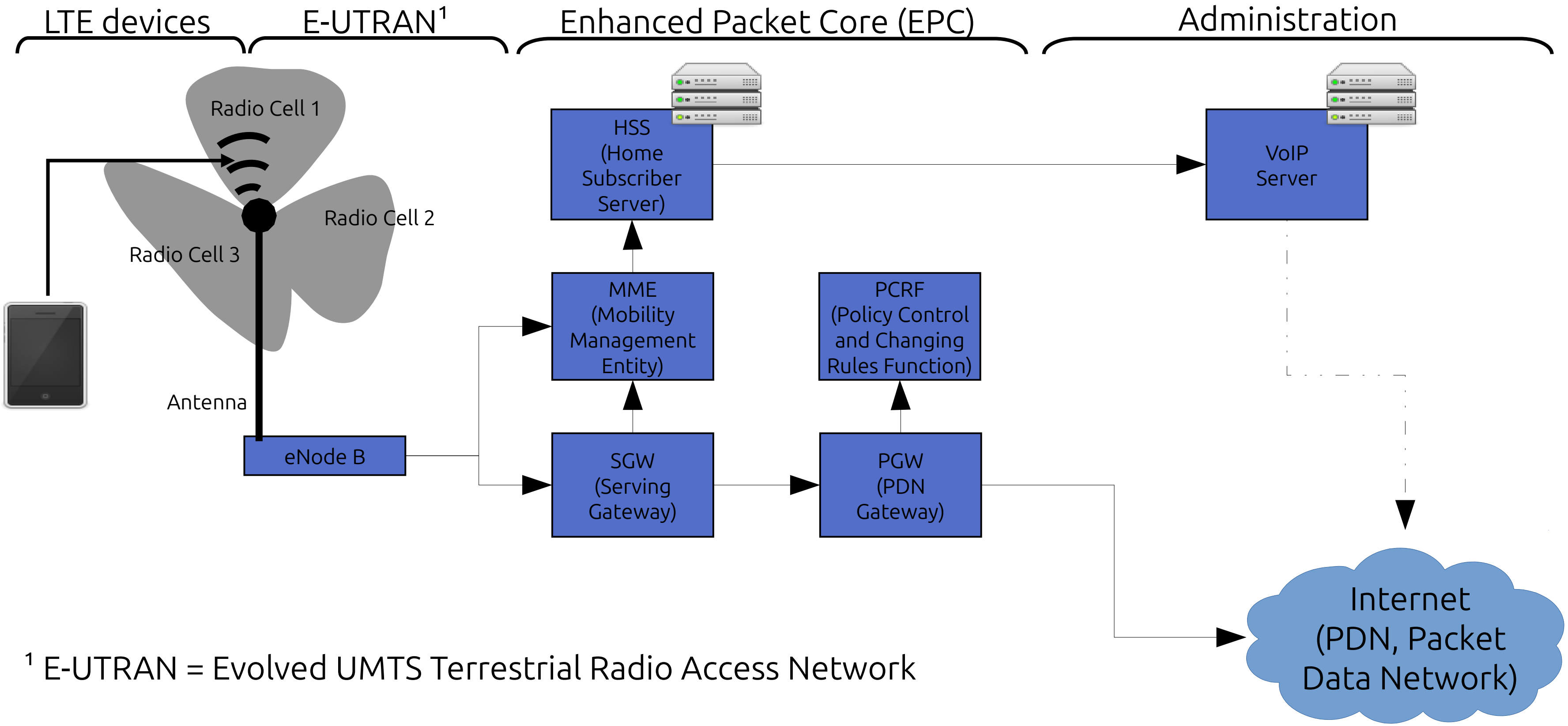
Phy = Physical layer
ATM = Asychronous Transfer Mode
AAL = ATM Adaptation Layer
UDP = User Datagram Protocol
TCP = Transmission Control Protocol

HTTP = Hypertext Transfer Protocol
AP = Application
RTP = Realtime Transfer Protocol
AMR = Adaptive Multi-Rate
SDP = Session Description Protocol

Standards: LTE (4G)

- Current de-facto WWAN standard
- Some aspects *less* complex than UMTS
  - Only packet-switched IP data
  - Also used for voice communication (Voice over IP)
- Most functionality still hidden from user

Standards: LTE network schema



[1] E-UTRAN = Evolved UMTS Terrestrial Radio Access Network

Standards: 5G

- Next WWAN standard
- Similar to 4G in many aspects (just faster):
  - Only packet-switched IP data
  - Also used for voice communication (Voice over IP)
- Also includes sub-standards for further scenarios:
  - Campus networks (large factories), alternative to WiFi
  - Low-bandwidth, long-range mode for IoT devices
  - Microcells for home or office deployment
  - Car-to-Car communication for future mobility

Standards: Summary

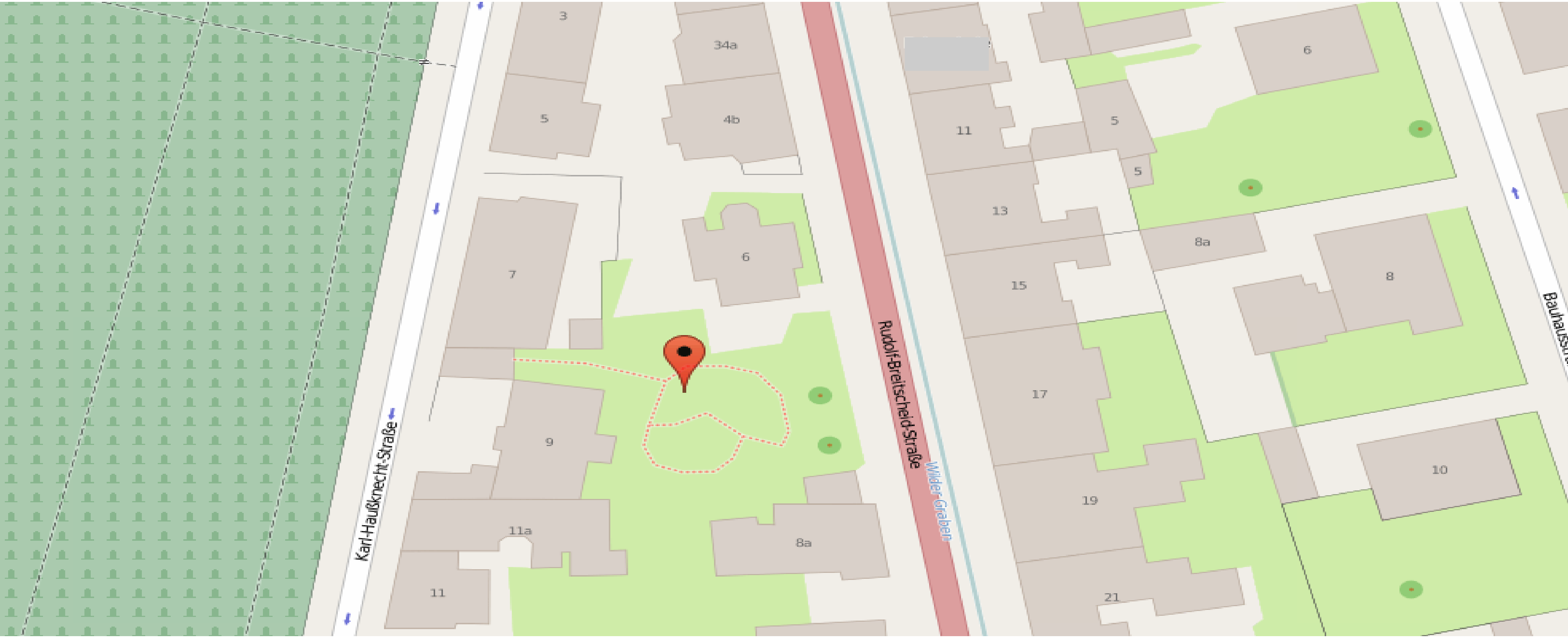
- Big “families” of wireless standards
  - WPAN: Bluetooth (all 7 ISO/OSI layers → complex)
  - WLAN: 802.11x (only lowest 2 layers)
  - WWAN: UMTS, LTE, 5G (also highly complex)
  - (LoRaWAN/LPWAN: see lecture 8)
- Sometimes overlap/interference between different sub-standards
  - Bluetooth and WiFi coexistence
  - 5G nudging into WiFi space

Location: Overview

- Objects & usage scenarios
- Classes of location information
- Location determination
  - Satellite-based
  - Network-based

Where am I?

Image source (ODbL): http://www.openstreetmap.org/export#map=19/50.97309/11.32747



Location: Classes (1)

- Geographic (latitude, longitude) – given in:
  - Degrees, hours, minutes, seconds (outdated)
  - Fraction of degrees (N 50.972921, W 11.326795)
- Topological (street address)
  - Many levels of detail possible
  - Europe, Germany, Weimar, Karl-Haußknecht-Str. 7
- Cell-based (ID of network cell)
  - MAC address & SSID of WLAN access point
  - ID number of current cell tower

Location: Classes (2)

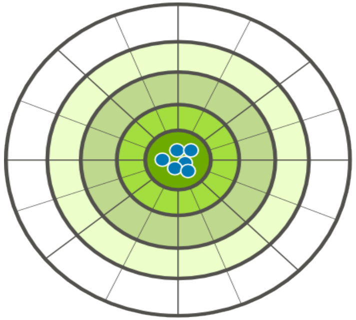
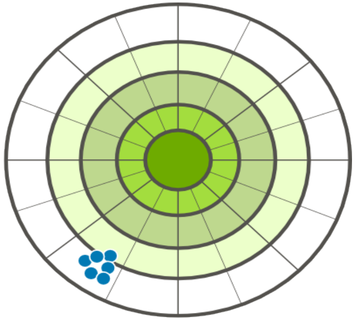
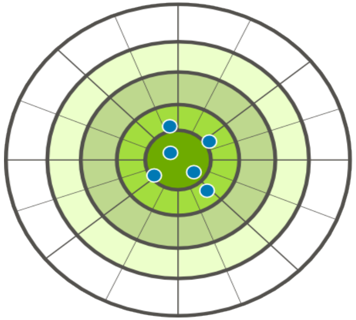
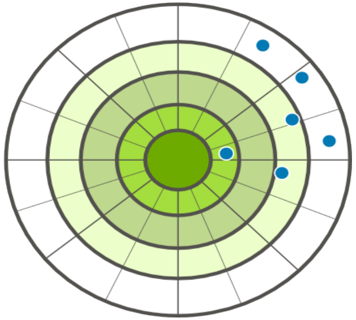
- Mapping between classes:
  - Topological → geographic: “geocoding”
    - E.g. map view: finding coordinates for street address
    - Usually graph database augmented with coordinates
  - Geographic → topological: “reverse geocoding”
    - “What address am I currently at?”
    - Requires “spatial index” on database → see GIS lecture
  - Cell ID → geographic/topological
    - Needs separate DB containing coordinates/addresses for access points & cell towers

Location: Methods

- Several types of "location providers" available in modern mobile devices
- Tradeoff: Accuracy ↔ battery consumption

Method	**Pro**	**Contra**
Satellites	+ Very accurate (~ 1 m)	- Works only outside - High power draw
WLAN cells	+ Lower power draw	- less accurate (~ 10 m)
Cell towers	+ No (additional) power draw	- quite inaccurate (~ 100 – 1000 m)

Location: Terminology

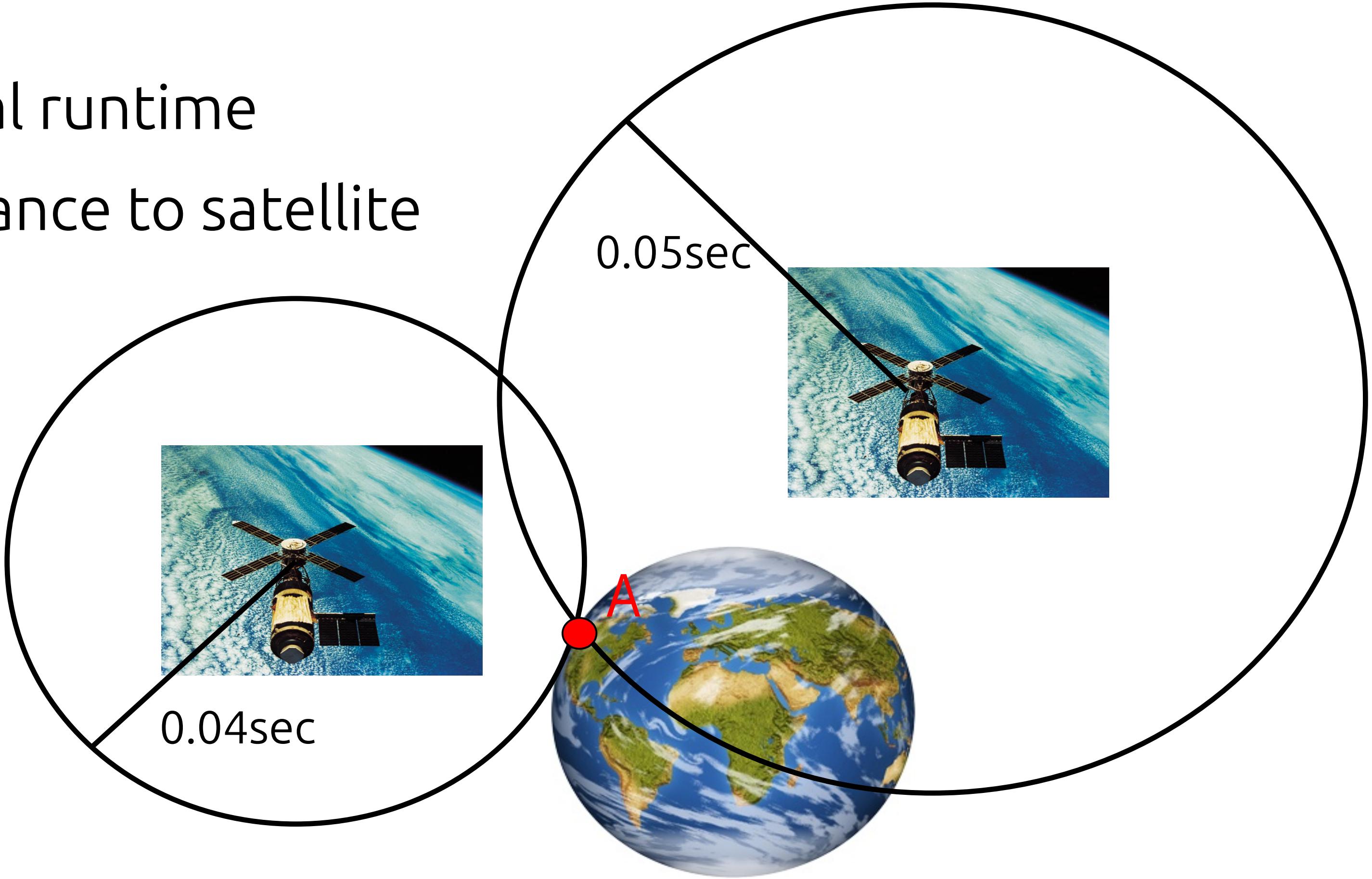
	High accuracy	Low accuracy (systematic error)
High precision		
Low precision (reproduction error)		

Location: GPS (satellite-based)

- 4 major satellite-based location systems:
  - GPS (USA), GLONASS (RU), Galileo (EU), BeiDou (CN)
  - Only Galileo under civilian control, others military
  - NavIC (IN) currently regional, planned expansion
- Following slides refer to GPS
  - Based on signal time-of-flight (TOF)
  - Very similar for GLONASS/Galileo/BeiDou
- Most modern mobile devices support all systems

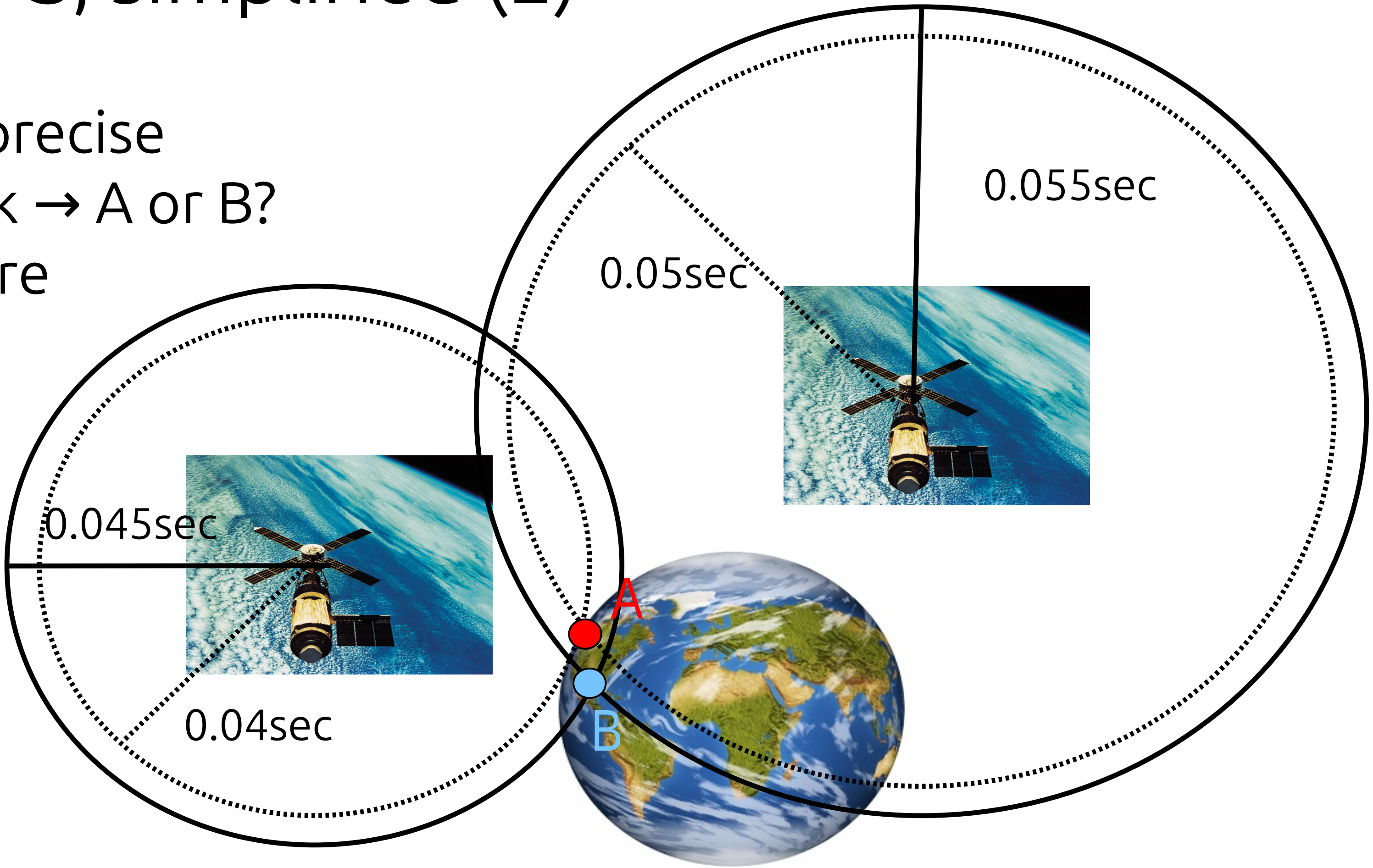
Location: GPS, simplified

- Measure signal runtime
- Calculate distance to satellite
- Intersect resulting circles (spheres)



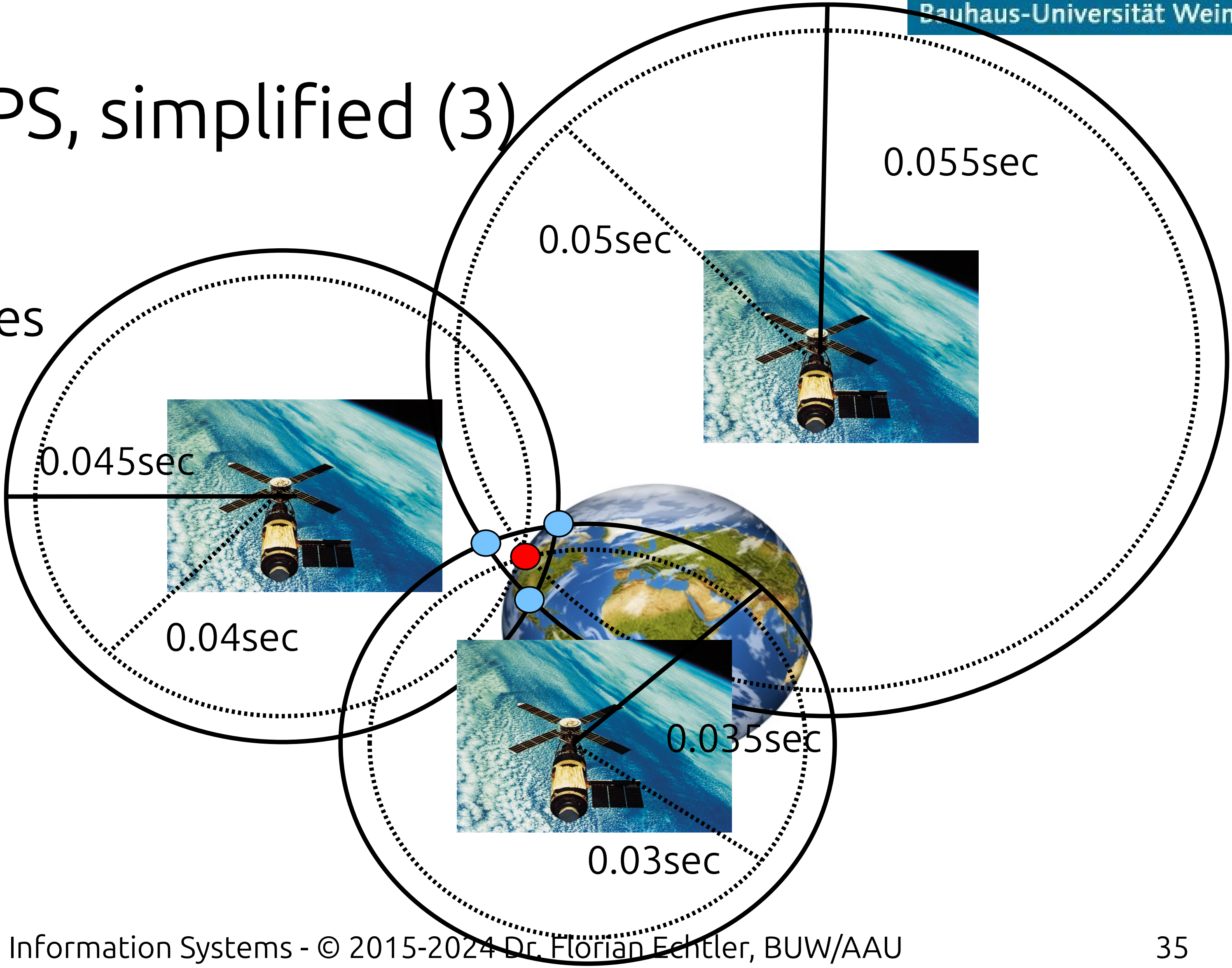
Location: GPS, simplified (2)

- Problem: imprecise receiver clock → A or B? Or somewhere in between?



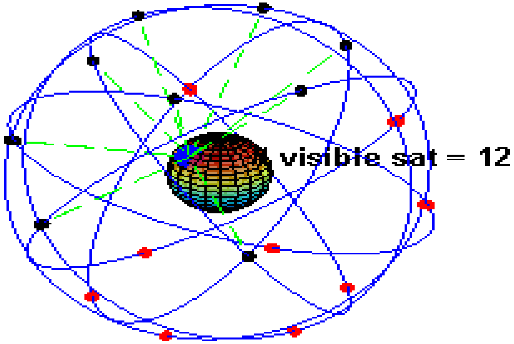
Location: GPS, simplified (3)

- Solution: use more satellites



Location: GPS – facts

Image source (PD): https://en.wikipedia.org/wiki/Global_Positioning_System#/media/File:ConstellationGPS.gif



- 32 satellites in operation, altitude ~ 20 000 km
- Equipped with high-precision atomic clocks (relativity!)
- At least 4 visible satellites required for position fix, usually 8 – 9 for any given point
- Position calculated using time *difference* of arrival (TDOA) instead of time of arrival (TOA) → no precision clock in receiver required

Location: GPS – facts (2)

- Signal characteristics:
  - Coarse/Acquisition (C/A) and Precision (P) code
  - Frequency bands 1575.42 MHz & 1227.60 MHz, effective bitrate 50 bits/second
  - Very low signal-to-noise-ratio (SNR) due to distance
- Contents of signal data:
  - Satellite clock & orbital data (“ephemeris”), required for position calculation
  - Constellation data (“almanac”), used to quickly “lock” onto satellite signal + improve precision

Location: GPS – extensions

- “Assisted” GPS (aGPS)
  - Almanac can be “side-loaded” via data connection
  - Improves time to first fix (TTFF) & precision
- Differential GPS
  - Add one or more stationary receivers
  - Use known position offset to improve accuracy of moving receivers

Location: GPS – coordinate systems

Image source (FU): https://en.wikipedia.org/wiki/...China_coordinate_system_misalignment.png

- Widely used: 1984 World Geodetic System (WGS-84)
  - Mapping from latitude/longitude to actual location on Earth
- Exception: China (uses GCJ-02, intentionally shifted vs. WGS)
  - Adds multiple sine waves as offset, for “security reasons”
  - Satellite images use WGS, street data uses GCJ → mismatch
  - Warning: Hongkong/Macau use WGS-84!

Location: GPS pro & contra

- Advantages
  - High accuracy, available all over the world
  - (Mostly) independent of external factors (weather)
- Disadvantages
  - Direct „line of sight“ to the satellites required
  - Cold start can be very slow (several minutes)
  - Running the system is expensive → ultimately still under military control, speed/altitude restrictions
  - Civilian use can be turned off (in theory)

Location: GPS - summary

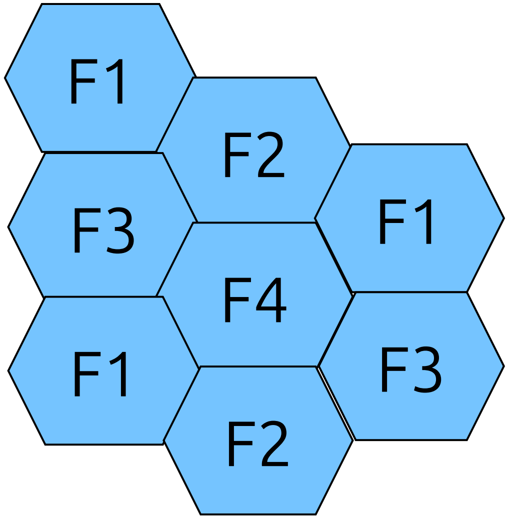
- Based on TDOA measurements to satellites
- Very precise, but high power draw & line-of-sight required
- Mostly under military control, except Galileo

Location: cell-based

- Basic idea:
  - Determine unique IDs of available network cells
    - WLAN: MAC address & SSID (network name)
    - WWAN: cell tower ID number
  - Use database to lookup coordinates of cells
- Depends on:
  - Database availability & quality
  - Cell size & shape
  - Signal quality

Location: cell-based – structure

- Cell shape: circular (theory), hexagonal (planning), irregular (reality)
- Neighbouring cells use different frequencies to minimize interference
- Some cell overlap inevitable
- Cell sizes:
  - WiFi: 10 m – 100 m
  - 3G/4G: 100 m – 5 km
  - 2G (GSM): 100 m – 35 km

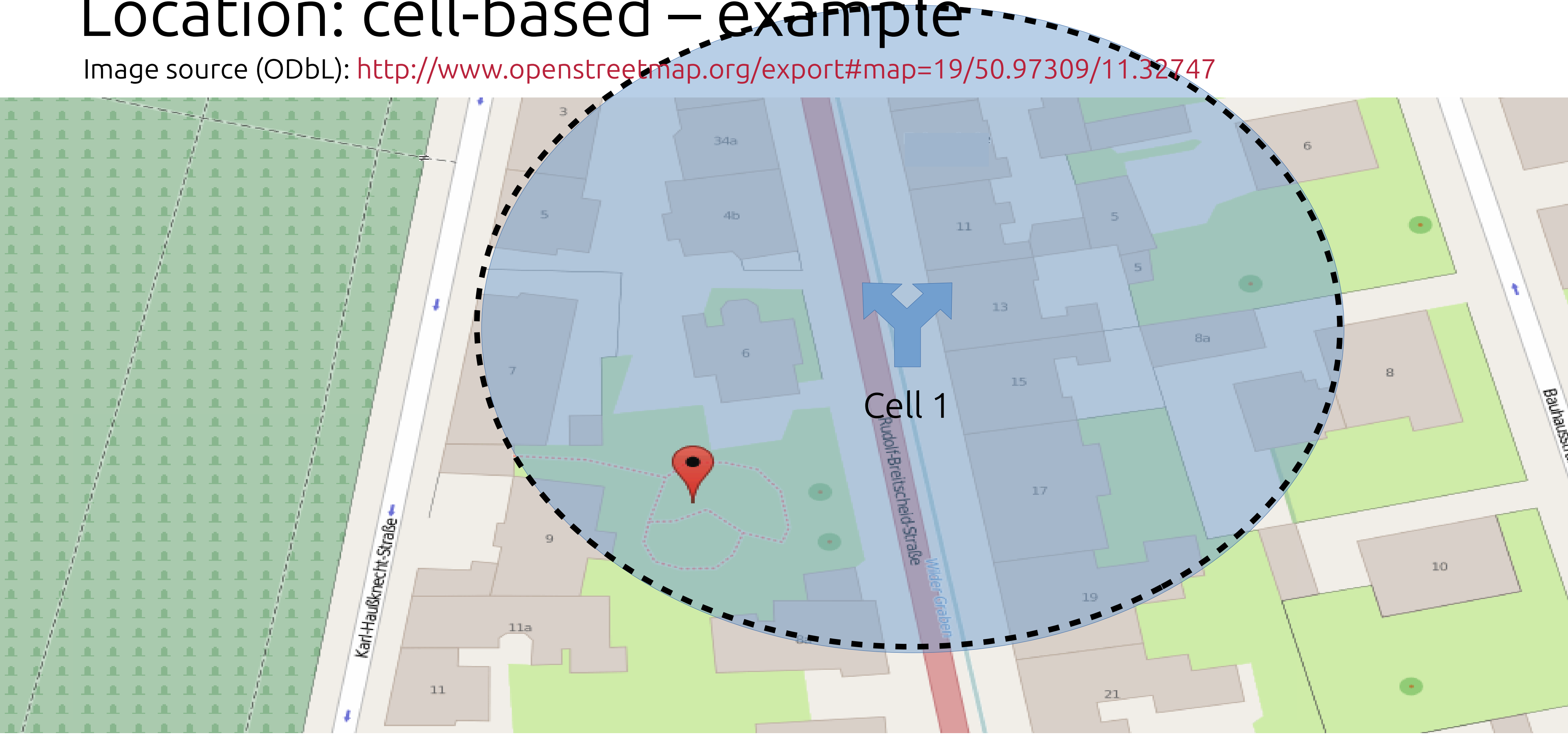


Location: cell-based – parameters

- Commonly used:
  - Currently used/logged-in cell
  - Cell sector (mostly for GSM/UMTS)
  - Other available cells
- Rarely used (why?):
  - Signal strength
  - Angle of arrival
  - Time difference, round-trip time

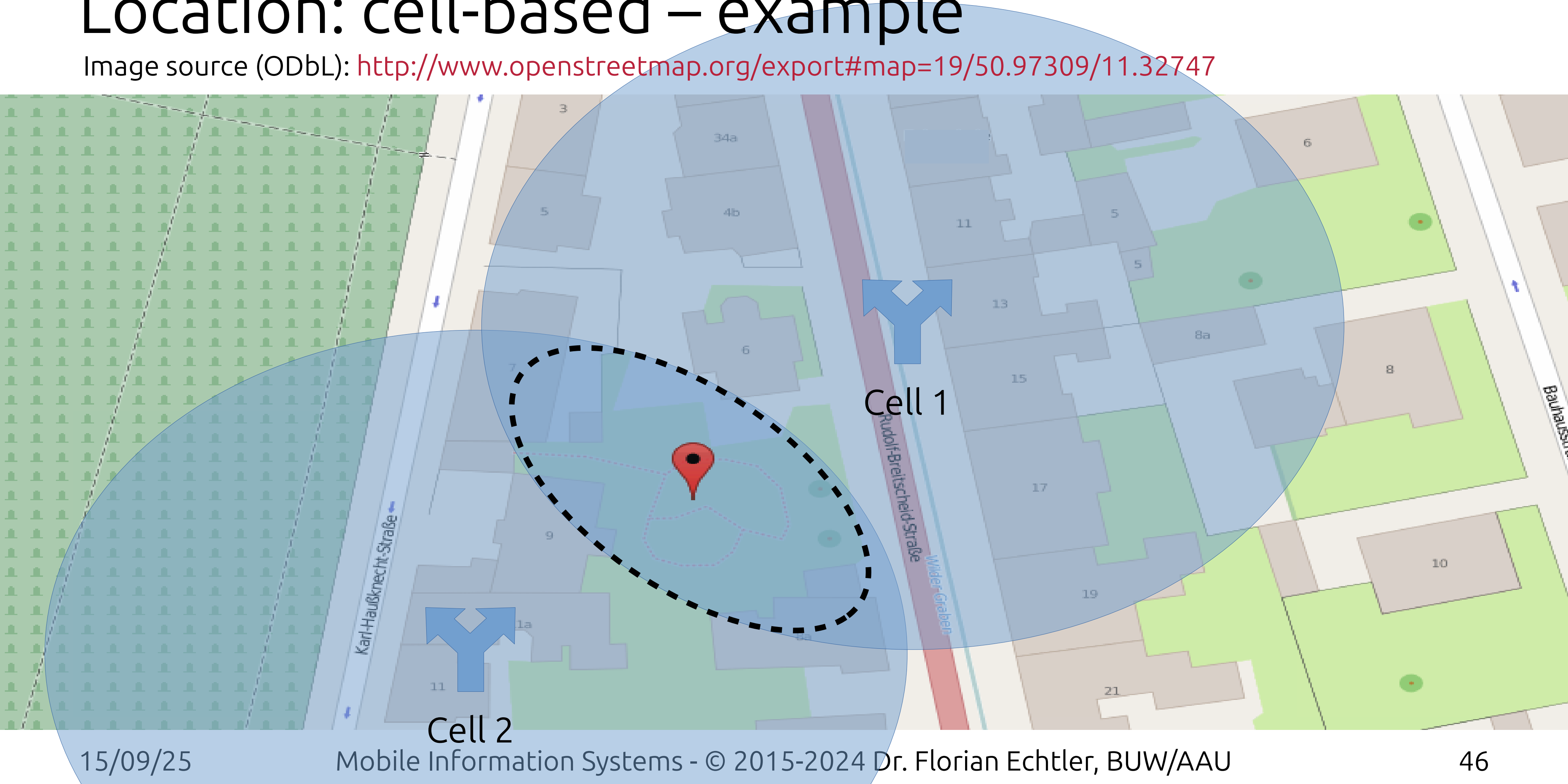
Location: cell-based – example

Image source (ODbL): http://www.openstreetmap.org/export#map=19/50.97309/11.32747



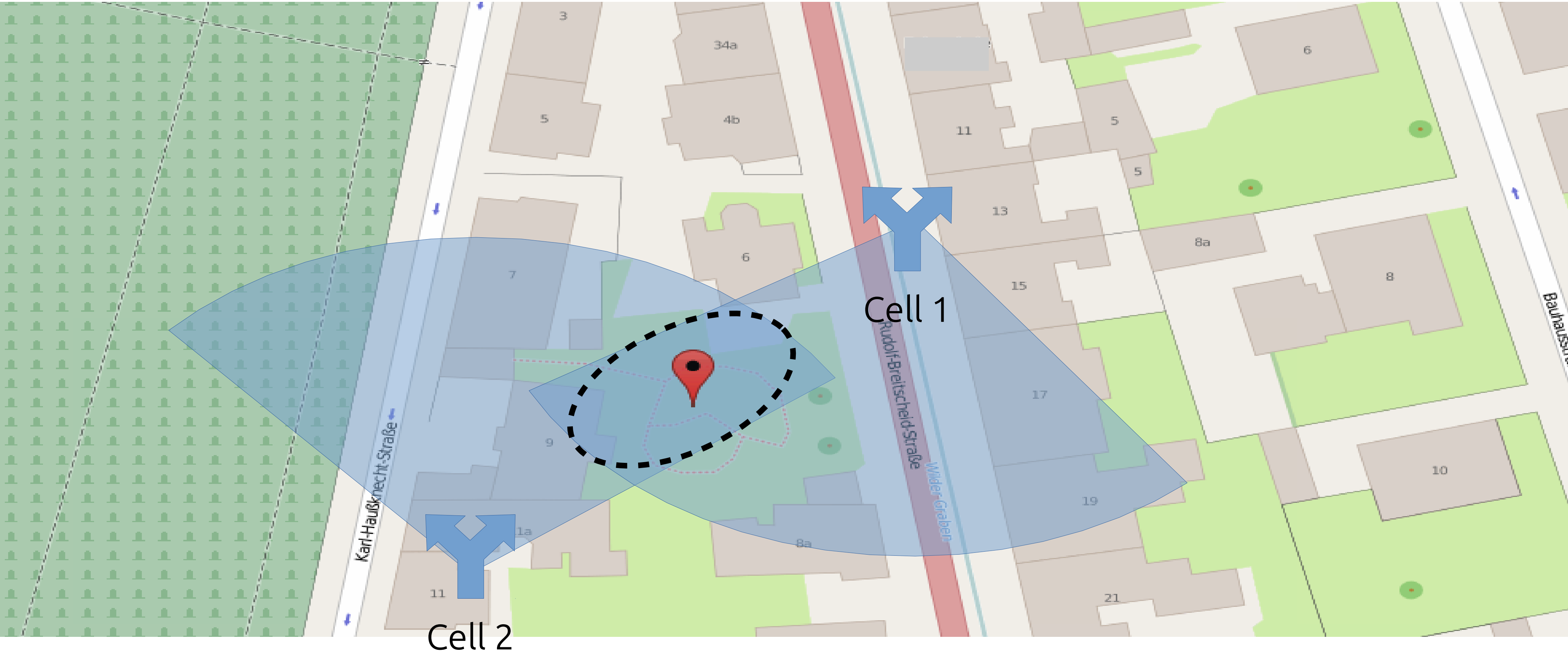
Location: cell-based – example

Image source (ODbL): http://www.openstreetmap.org/export#map=19/50.97309/11.32747



Location: cell-based – example

Image source (ODbL): http://www.openstreetmap.org/export#map=19/50.97309/11.32747



Location: cell-based – issues

- ~ 99% of queries use Google location database
  - access is logged → used to improve DB,
    but raises privacy issues
  - Alternatives (less coverage & accuracy):
    - OpenCellID
    - Mozilla Location DB
- Not available when offline, cell DB too large
- WLAN cells can move/change quickly
  → frequent updates required

Location: cell-based - Summary

- Less precise than GPS, but less power draw
- Quality depends mostly on …
  - Cell size & shape
  - Database coverage & access
- Privacy issues?

The End


SECURITY SAYS YOUR EMPLOYEE LOCATOR DEVICE ISN'T TURNED ON.
MY WHAT?
I THINK YOU CALL IT A SMART-PHONE.
I MIGHT HAVE SOME QUESTIONS.
PUT THEM IN A TEXT TO YOUR-SELF. I'LL READ THEM LATER.
Dilbert.com DilbertCartoonist@gmail.com
5-27-11 ©2011 Scott Adams, Inc.