CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

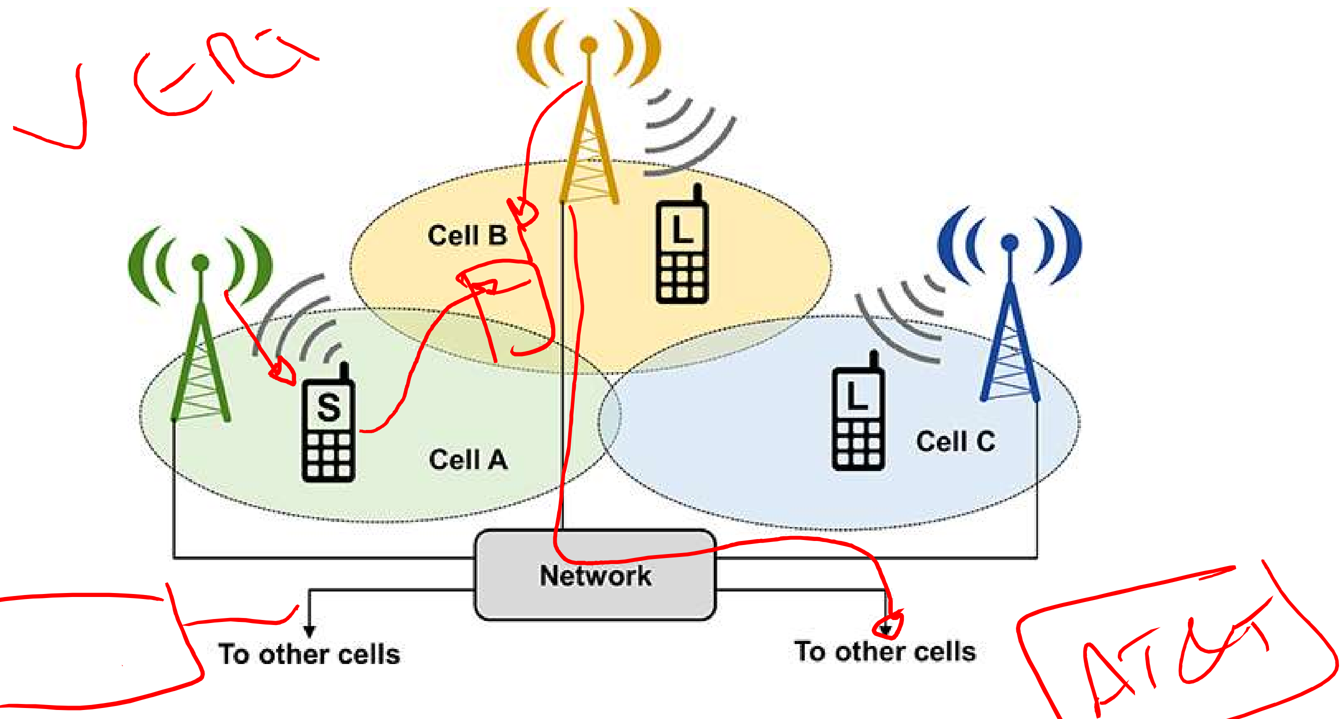
Wireless, IoT, and Cloud Security

Introduction to Cellular Networks

Video summary

- Introduction to Cellular Networks
- Cellular Networks Generations
- Introduction to GSM 2G
- GSM Security Aspects

Cellular Communication Systems



- When moving between two cells, the cellphone must handover from one BS to the other.

Cellular Communication Systems (cont'd)

Planning

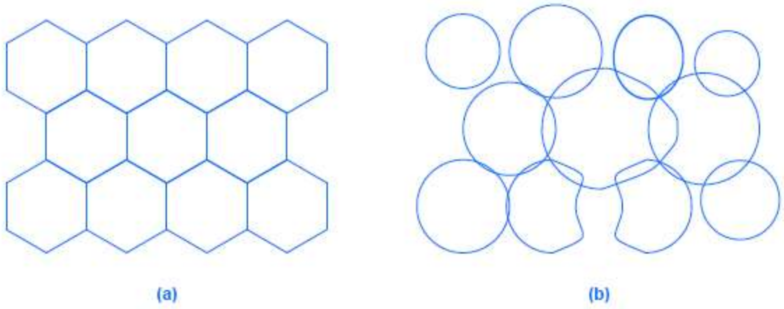
(a) Perfect cellular coverage occurs if each cell is a hexagon:

- because the cells can be arranged in a honeycomb
- in practice, cellular coverage is imperfect

(b) Most cell towers use omnidirectional antennas:

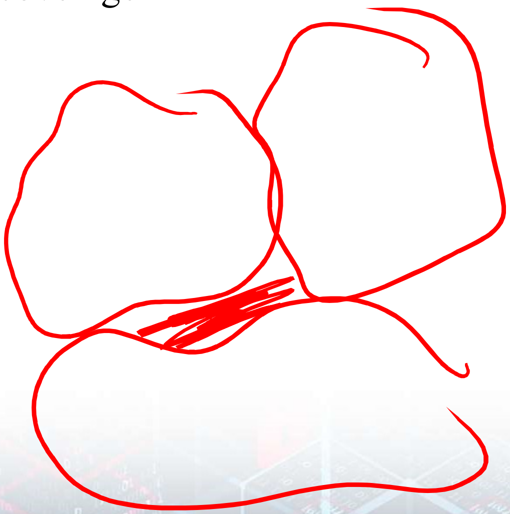
- transmit in a circular pattern
- obstructions and electrical interference can attenuate a signal or cause an irregular pattern
  - in some cases, cells overlap and in others, gaps exist with no coverage

✓



(a)

(b)



Generations of Cellular Technologies

Telecommunications industry divides cellular technologies into four generations: 1G, 2G, 3G, and 4G (with intermediate versions labeled 2.5G and 3.5G)

Simplified Descriptions:

1G

- Began in the late 1970s, and extended through the 1980s
- Originally called cellular mobile radio telephones
- used analog signals to carry voice

2G and 2.5G

56 kbps

- Began in the early 1990s and continues to be used
- One standard: GSM (General System for Communications)
- The main distinction between 1G and 2G arises because 2G uses digital signals to carry voice
- The label 2.5G is used for systems that extend a 2G system to include some 3G features

128 Kbps

Generations of Cellular Technologies (cont’d)

3G and 3.5G

- Began in the 2000s
- Focuses on the addition of higher-speed data services
- A 3G system offers download rates of 400 Kbps to 2 Mbps, and is intended to support applications such as web browsing and photo sharing
- Includes EDGE (Enhanced Data Rates for GSM Evolution)

4G and 4G LTE (Long Term Evolution)

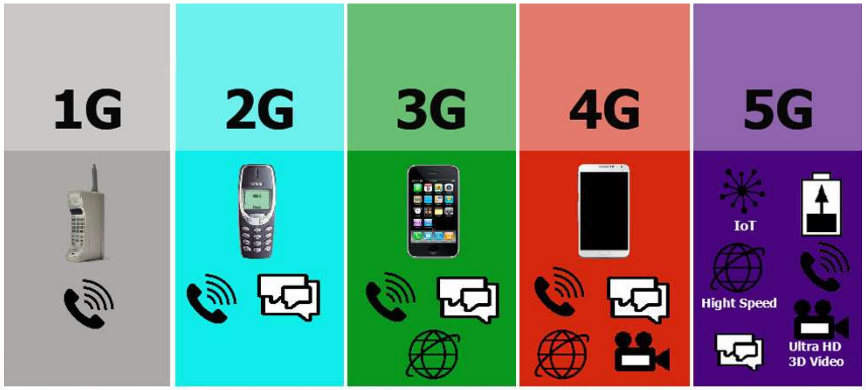
- Began around 2008
- Higher data rate up to 20 Mbps
- Focuses on support for real-time multimedia
    - such as a IPTV
- They include multiple connection technologies
    - such as Wi-Fi and satellite

Generations of Cellular Technologies (cont’d)

5G

1 Gbps

- Began in the 2018 - 2019
- Very high speed data service (Gbps)
- Focus on low latency applications (< 1 ms)
- Focus on Massive device connectivity (Up to 100x number of connected **devices** per unit area)
- 99.999% availability.
- 90% reduction in **network** energy usage.



GSM 2G

➢Global System for Mobile Communications

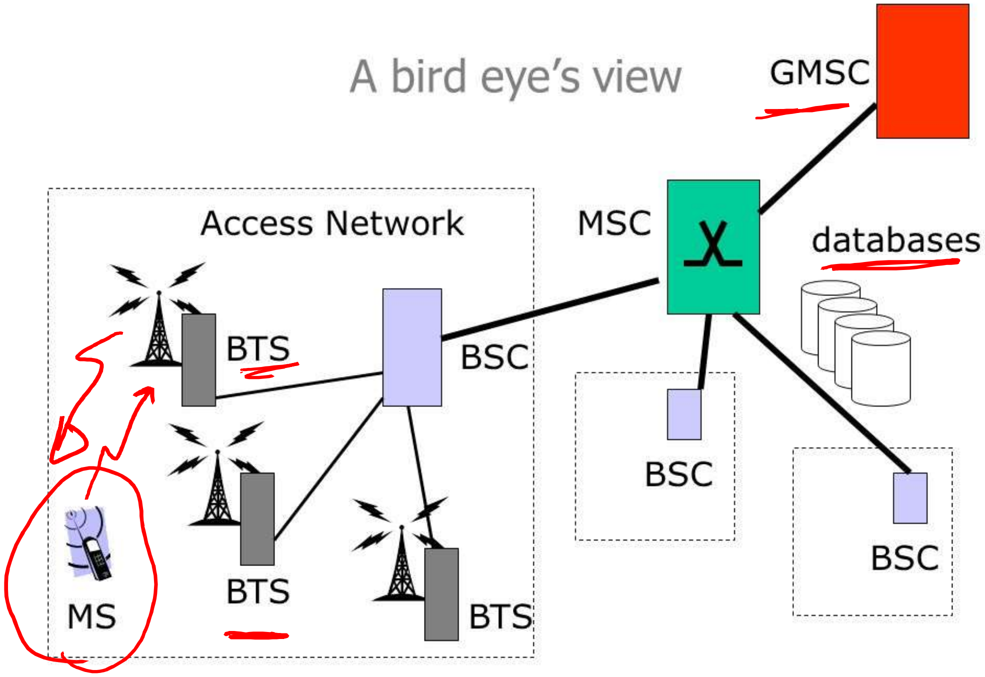
- GSM is the most popular standard for mobile phones
- The GSM Association estimates 82% of the global mobile market uses this standard
- Two billion people across more than 200 countries used GSM

➢Services

- Voice Communication, Short Messaging Service, …etc.

Digital

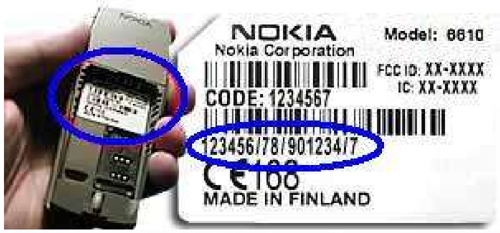
Architecture of GSM



Mobile Station

- Mobile Equipment
  - International Mobile Equipment Identity (IMEI)

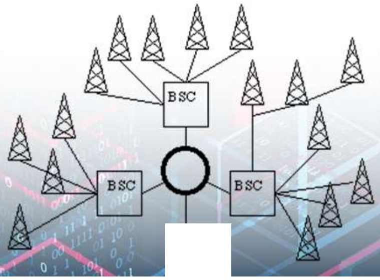
- Subscriber Identity Module (SIM) card
  - Smart Card containing identifiers, keys and algorithms



Base Station Subsystem

- Base Transceiver Station (BTS)
  - A cell is formed by the radio coverage of a BTS
  - Provide the radio channels and handle the radio-link protocol

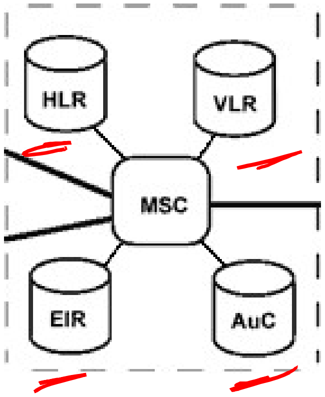
- Base Station Controller (BSC)
  - Manage the radio resources for one or more BTS
  - Handle channel setup and handovers
  - Connect to the mobile service switching center



Network Subsystem

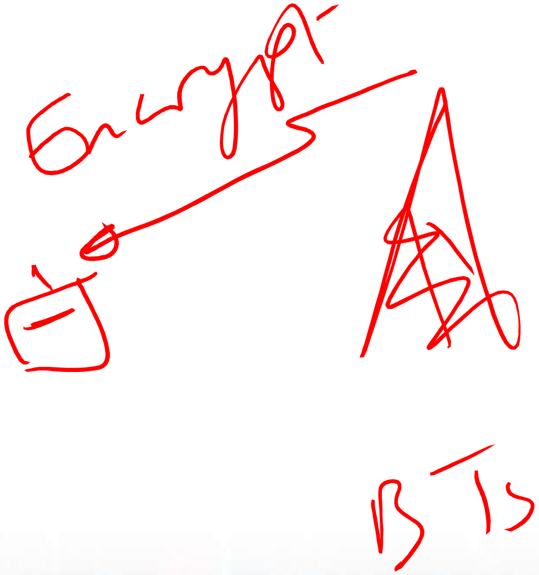
IMSI Black list

- Components in Network Subsystem
  - MSC: Mobile services Switching Center
  - HLR: Home Location Register
  - VLR: Visitor Location Register
  - AuC: Authentication Center
  - EIR: Equipment Identity Register
- Network Subsystem features
  - Telephone switching function
  - Subscriber profile
  - Mobility management



GSM Basic Security Goals

- Subscriber Authentication to protect the operator against the billing fraud
- Confidentiality on the radio path
- User Anonymity
- Lower overhead introduced by security mechanisms



GSM Security Aspects

- Subscriber authentication
  - The operator knows for billing purposes who is using the system
- Subscriber identity confidentiality
- User data confidentiality
- Key management
- Detection of compromised equipment

SIM card (Subscriber Identity Module)

- Removable from the Mobile Station

- Contain all data specific to the end user which have to reside in the Mobile Station:
  - IMSI: International Mobile Subscriber Identity (user’s permanent identity)
  - PIN – Personal Identity Number protecting a SIM
  - TMSI (Temporary Mobile Subscriber Identity)
  - K_i : User’s secret key
  - K_c : Ciphering key
  - LAI – location area identity
  - List of the last call attempts, List of preferred operators, Supplementary service data (abbreviated dialing, last short messages received,...)

Key Management Scheme

- **K_i** – Subscriber Authentication Key
  - Shared 128 bit key used for authentication of subscriber by the operator
  - Key Storage
    - Subscriber’s SIM (owned by operator, i.e. trusted)
    - Operator’s Home Locator Register (HLR) of the subscriber’s home network

Authentication

➢Authentication Goals

- Subscriber (SIM holder) authentication, protection of the network against unauthorized use
- Create a session key for the next communication

Ki

➢Authentication Scheme

- Subscriber identification: IMSI/TMSI
- Challenge-Response authentication of the subscriber
- Long-term secret key shared between the subscriber and the home network
- Supports roaming without revealing long-term key to the visited networks

Video summary

- Introduction to Cellular Networks
- Cellular Networks Generations
- Introduction to GSM
- GSM Security Aspects