Wireless Cellular Network Security: Part 1

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

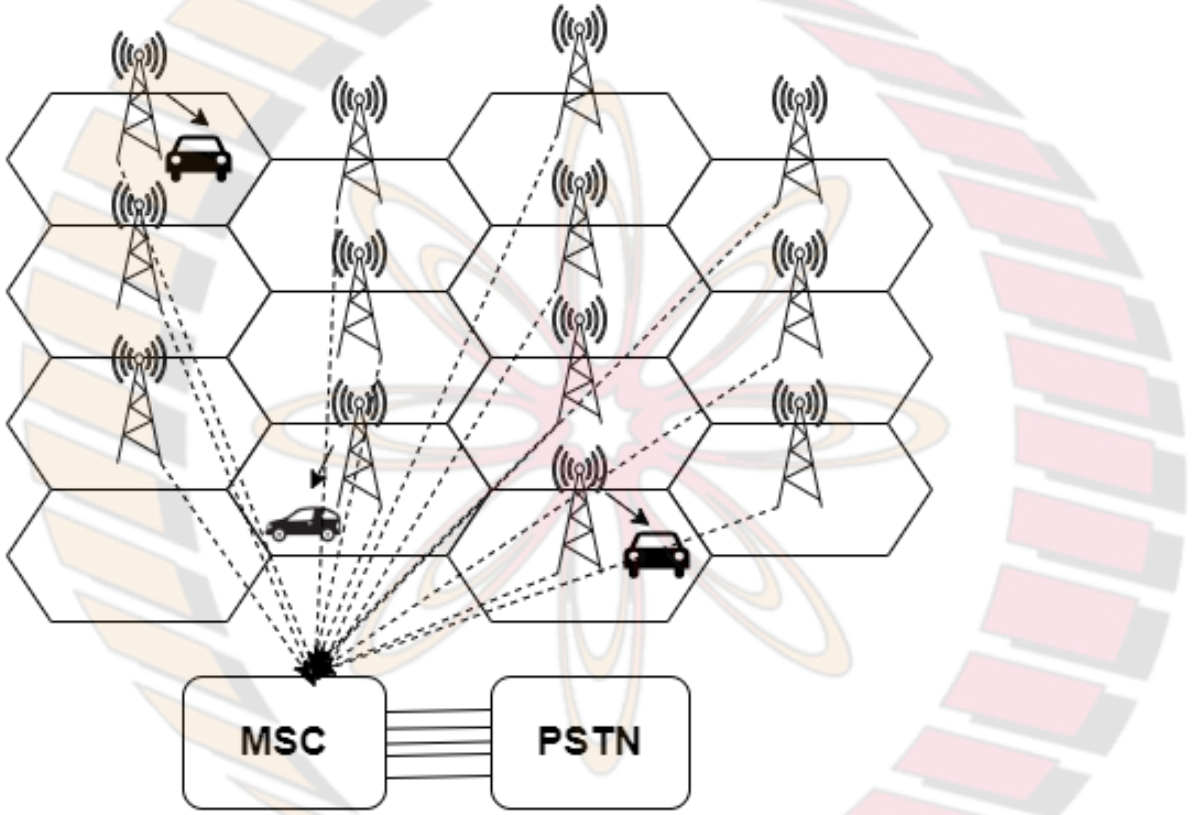
References

- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt. Ltd., 2018
- T.S. Rappaport, "*Wireless Communications: Principles and Practice*", Prentice Hall of India, 2nd ed, 2002.

Recall: Wide-Area Wireless Access

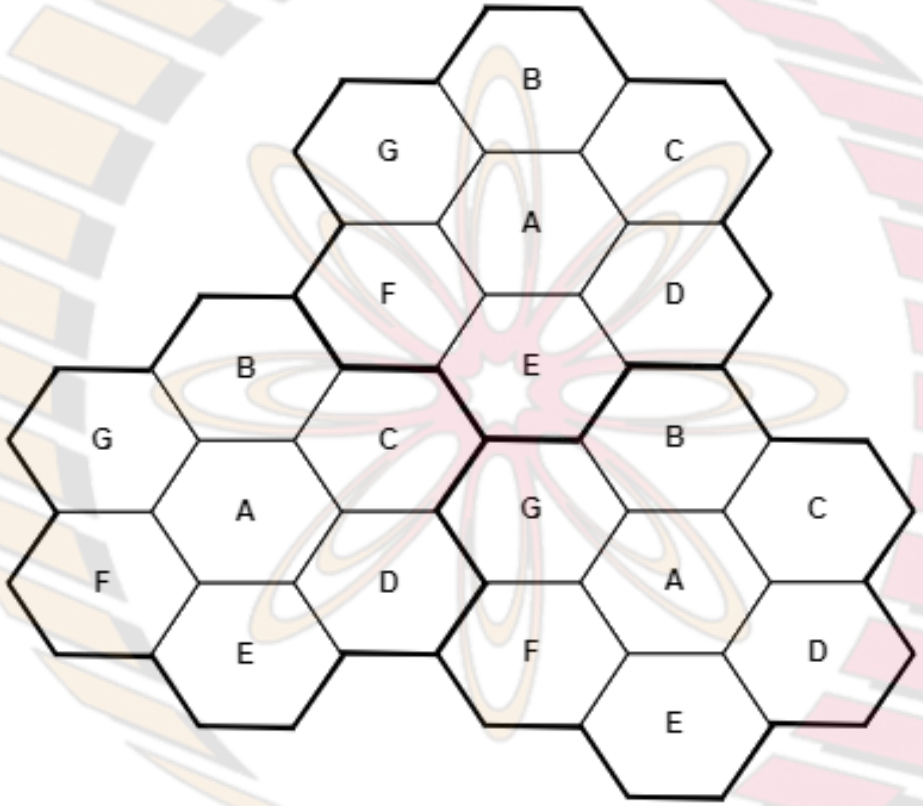
- Cellular networks (*e.g.*, 2G, 3G, 4G, 5G)
  - Internet and telephone connectivity in mobile phones throughout large region (*e.g.*, city)
- **Speeds**: few 10s of Mbps to several Gbps
- **Wireless**: shared medium
  - MAC protocol needed
- Deployed by cellular operators (*e.g.*, Airtel, Vi)
- Spectrum needs to be *licensed* from regulator
  - costly, but exclusive access

Recall: Cellular Network Architecture



- Region (*e.g.*, city) divided into small areas called "*cells*"
  - ❑ typically cell radius < 5 km
- Each cell served by one BS

Recall: Frequency Reuse



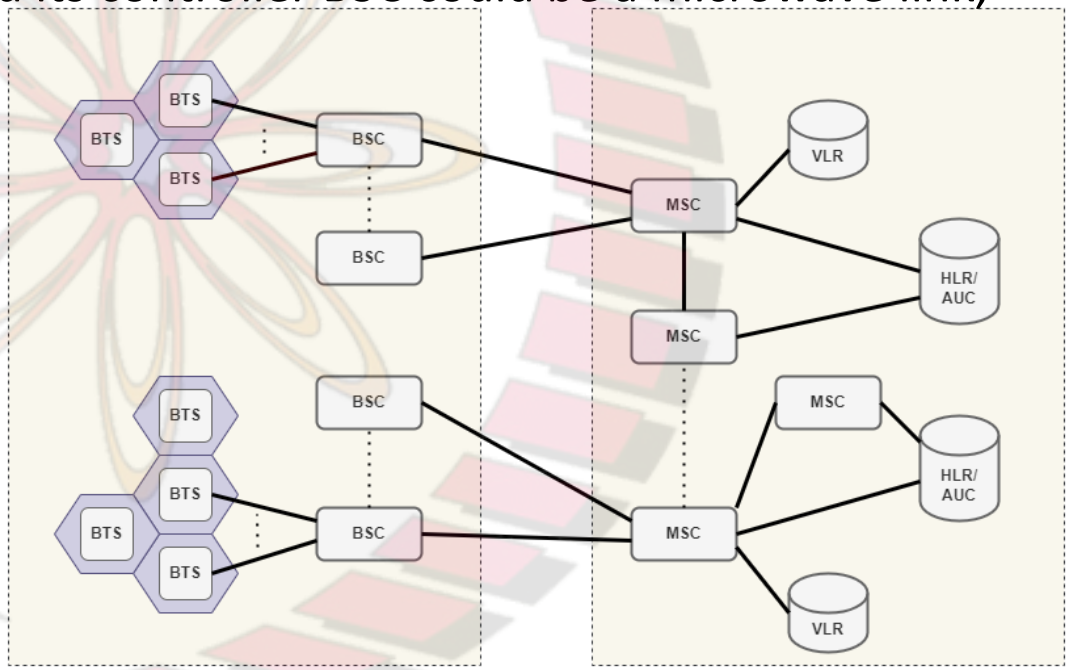
- *Same set of frequencies used at far-apart cells without mutual interference*
- Increases capacity of system

2G and 3G Cellular Networks

- One of the most popular second-generation (2G) cellular networks:
  - Global System for Mobile Communications (GSM)
- Provided several advantages over analog (1G) cellular networks:
  - Better voice quality
  - Higher speeds for data and other non-voice applications
  - International roaming
- From a security viewpoint: was designed to protect against:
  - Eavesdropping
  - Intruder masquerading as a legitimate mobile phone user
- Successor to GSM was Universal Mobile Telecommunications System (UMTS), a 3G technology
- UMTS provided advanced services, e.g.:
  - mobile Internet
  - multimedia messaging
  - videoconferencing, etc.
- Security provided in GSM is significantly better than that in 1G cellular networks
- However, GSM security still had several shortcomings, which were overcome in UMTS networks
- Next: we study the security mechanisms available in both 2G and 3G

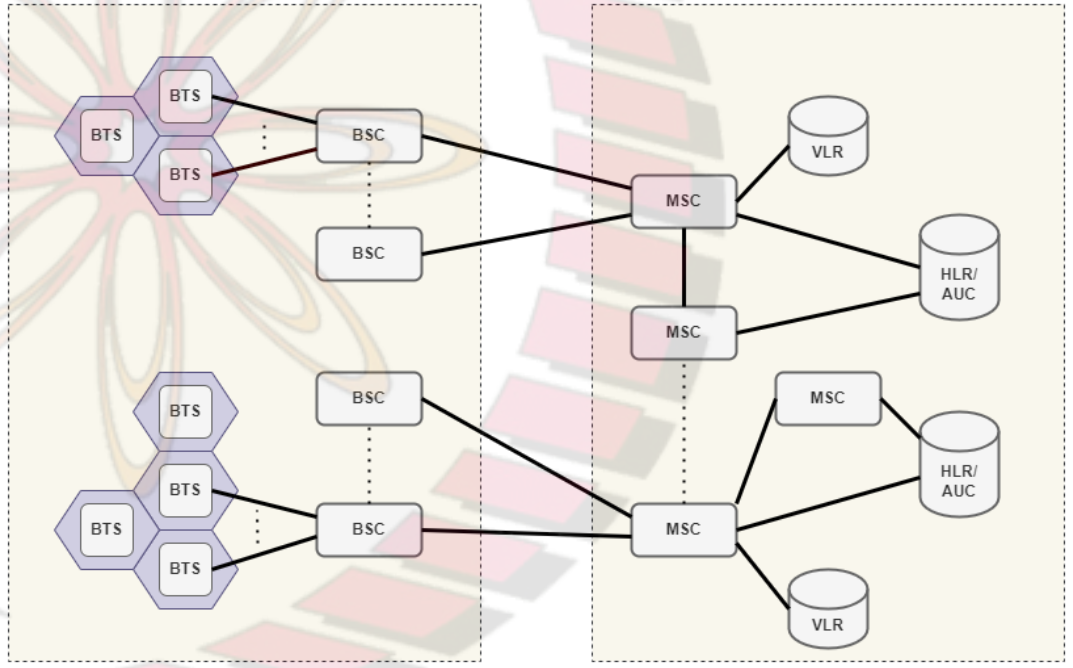
2G and 3G Network Architecture

- Cellphone is wirelessly connected to a base station or base transceiver station (BTS)
- Multiple BTSs are, in turn, connected to and controlled by a base station controller (BSC)
  - ❑ connection between a BTS and its controller BSC could be a microwave link, optical link, etc.
- Multiple BSCs are connected to a Mobile Switching Centre (MSC)
- MSC forwards an incoming call to the MSC where the call recipient is located
- MSC also handles call billing and accounting functions
- MSCs connected to each other through wired networks such as Packet Switched Telephone Network (PSTN)



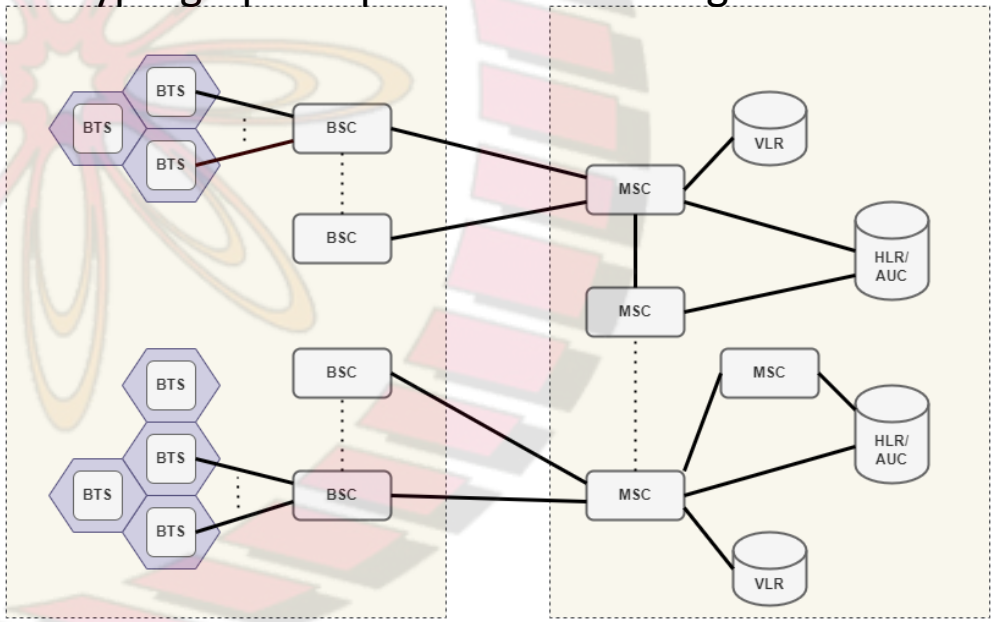
2G and 3G Network Architecture (contd.)

- A user's home network is the one with whom the user has a subscription
  - ❑ "a network" is the part of the overall network managed by a particular MSC
- MSC has a database containing information about each of its subscribers:
  - ❑ called Home Location Register (HLR)
- This information includes static information, e.g.:
  - ❑subscriber's mobile number, services subscribed to
  - ❑secret key stored in the mobile and known only to the HLR
- HLR also contains dynamic information for each of its roaming subscribers
  - ❑ this includes current location of a subscriber, i.e., the cellular network the user may be currently visiting



2G and 3G Network Architecture (contd.)

- A subscriber may avail of the services of other ("foreign") networks that have a roaming agreement with the subscriber's home network
- Each cellular network also maintains a database of users currently visiting that network together with the list of services the subscriber is entitled to
  - ❑ referred to as Visitor Location Register (VLR)
- 2G technology introduced the idea of a Subscriber Identity Module (SIM) card
  - ❑ A smart card that can be removed from one cellphone and placed in another
- SIM card stores three secrets and performs cryptographic operations involving some of these secrets
- The secrets are:
  - ❑ A unique 15-digit subscriber identification number called the International Mobile Subscriber Identity (IMSI)
  - ❑ A 128-bit subscriber authentication key, K_i, known only to the SIM and the HLR of the subscriber's home network
  - ❑ A PIN known to the phone's owner and used to unlock the SIM
    - Intended to prevent stolen phones from being used
    - This feature rarely used in practice



2G and 3G Security Goals

- Main security goals in GSM and UMTS are similar to those in wired networks, viz., authentication, integrity, and confidentiality
- User identity confidentiality:
  - One way for an eavesdropper to identify a caller is through the IMSI transmitted by the cellphone when a call is made
  - To protect user privacy, GSM requires that the IMSI be used rarely, e.g., during initial authentication to a foreign network
  - Instead, a Temporary Mobile Subscriber Identity (TMSI) is assigned to a user
  - TMSI has limited-time validity and, that too, only within a particular network
  - When a user changes location and moves to a new network, the user's cellphone will have to be re-authenticated and a new TMSI assigned
  - Mapping between a cellphone's TMSI and its IMSI is maintained in the VLR
  - Unlike the IMSI, which is a fixed subscriber ID, the TMSI is a random integer and its use is temporary
  - Hence, use of TMSI instead of IMSI helps prevent tracking of cellphone users

2G and 3G Security Goals (contd.)

- Message Confidentiality:
  - user data messages and some signalling messages need to be kept confidential
- Entity Authentication:
  - MSC needs to be sure that the call is billed to the person making the call
  - Also, caller needs to convince itself that it is talking to the genuine base station
- Message Integrity:
  - message integrity of signalling messages exchanged between the cellphone and the base station need to be achieved