Wireless Cellular Network Security: Part 4

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi, "*LTE Security*", John Wiley and sons, 2nd edition, 2013.

LTE (4G) Security

Introduction

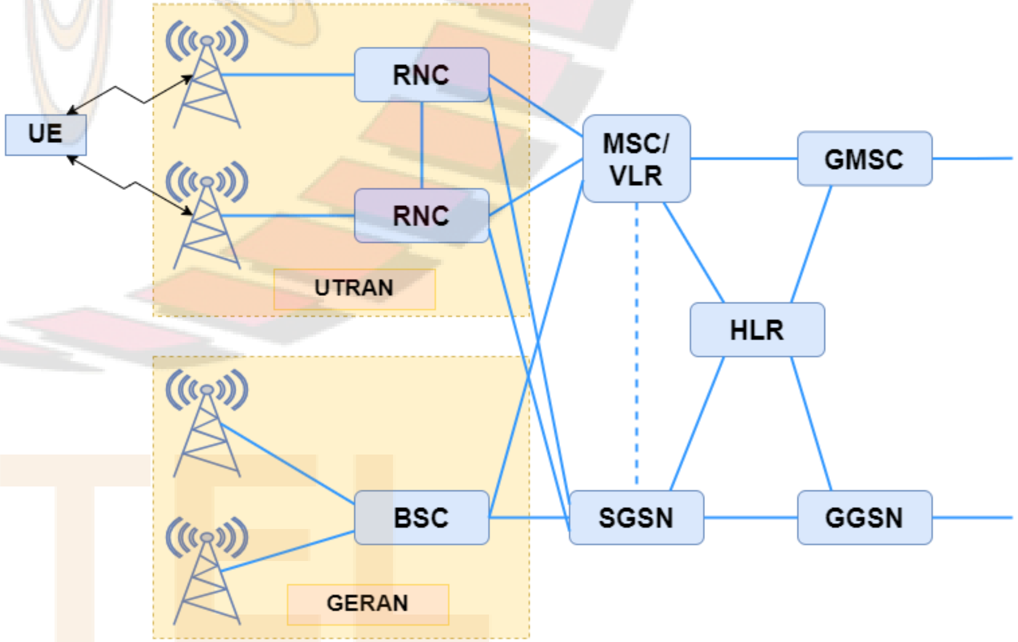
- Architecture of Long Term Evolution (LTE) cellular networks (4G) significantly different from those of 2G and 3G networks
- Also, several differences between security in LTE and in 2G and 3G cellular networks
- First, we provide an overview of:
  - ❑those aspects of architecture of 2G and 3G cellular networks, which we did not discuss earlier, but are relevant to 4G networks
  - ❑architecture of 4G cellular networks
- Then, we discuss security in 4G cellular networks

Evolution of Cellular Networks

- Both GSM and 3G systems were divided into two different domains, based on underlying switching technology:
    - ❑circuit-switched (CS) domain was mainly intended for carrying voice and short messages
    - ❑packet-switched (PS) domain was mainly used for carrying data traffic
- In contrast, Evolved Packet System (EPS) (technical name of 4G cellular network) contains only a PS domain
- MAC protocol used based on FDMA:
    - ❑Orthogonal Frequency Division Multiple Access (OFDMA) for downlink traffic
    - ❑Single Carrier Frequency Division Multiple Access (SC-FDMA) for uplink traffic

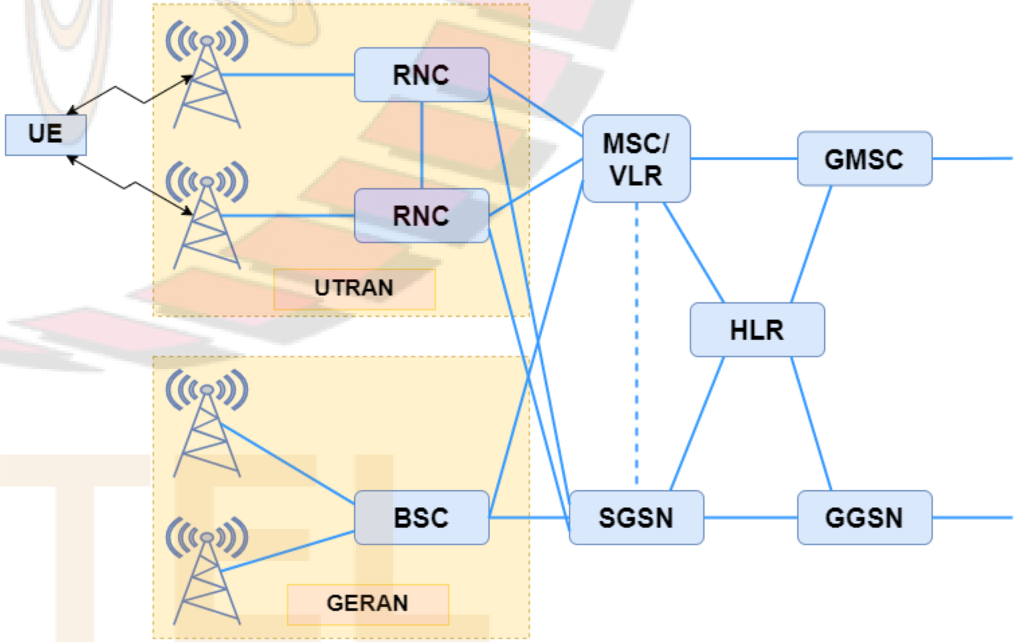
Overview of 3G Architecture

- User equipment (UE), i.e., mobile station, is wirelessly connected to Radio Access Network (RAN), which is connected to Core Network (CN)
- CN contains PS domain and CS domain:
  - ❑ PS domain is an evolution of the General Packet Radio Service (GPRS) domain of the GSM system, and its most important network elements are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN)
  - ❑ CS domain is an evolution from the original CS GSM network, with the Mobile Switching Centre (MSC) as its most important component
- Protocols involving the UE are grouped into two main strata:
  - ❑ Access Stratum (AS) contains protocols that are run between the UE and the access network
  - ❑ Non-Access Stratum (NAS) contains protocols between the UE and the CN



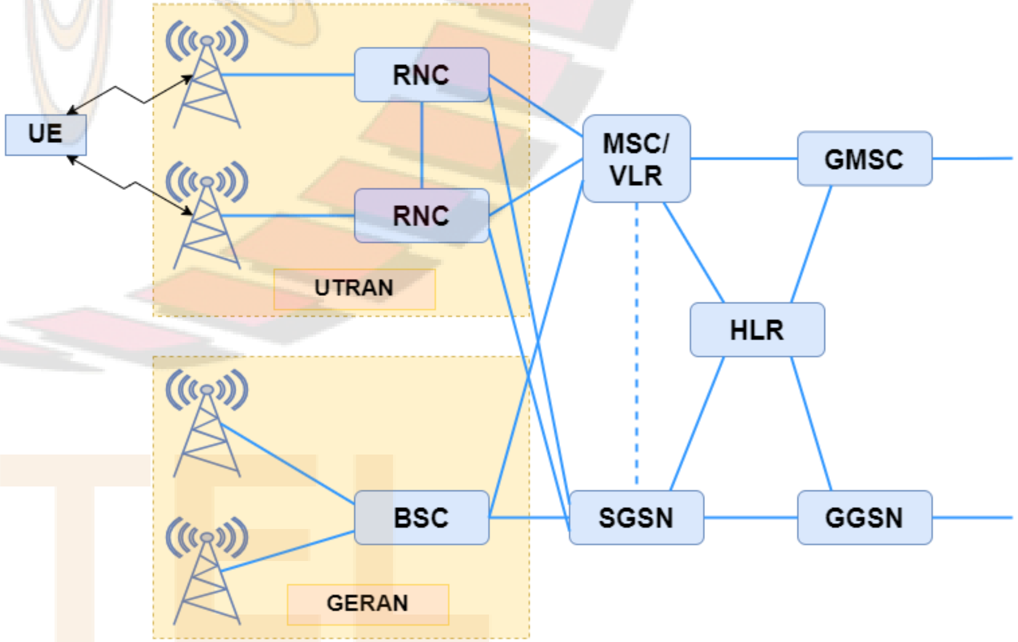
Overview of 3G Architecture (contd.)

- CN is further divided into:
  - ❑ the home network, which contains all the static information about the subscribers, including the static security information, and
  - ❑ the serving network, which handles the communication to the UE (via the access network)
- The UE consists of two parts:
  - ❑ Mobile Equipment (ME) and
  - ❑ Universal Subscriber Identity Module (USIM)
- Two types of RAN in the 3G system:
  - ❑ UMTS Terrestrial Radio Access Network (UTRAN) is based on WCDMA technology and
  - ❑ GSM/EDGE Radio Access Network (GERAN) is an evolution of GSM technology
- The BS is called:
  - ❑ Node B in the case of UTRAN and
  - ❑ Base Transceiver Station (BTS) in GERAN
- The BS is connected to the controlling unit of the RAN, which is the:
  - ❑ Radio Network Controller (RNC) in UTRAN or the
  - ❑ Base Station Controller (BSC) in GERAN



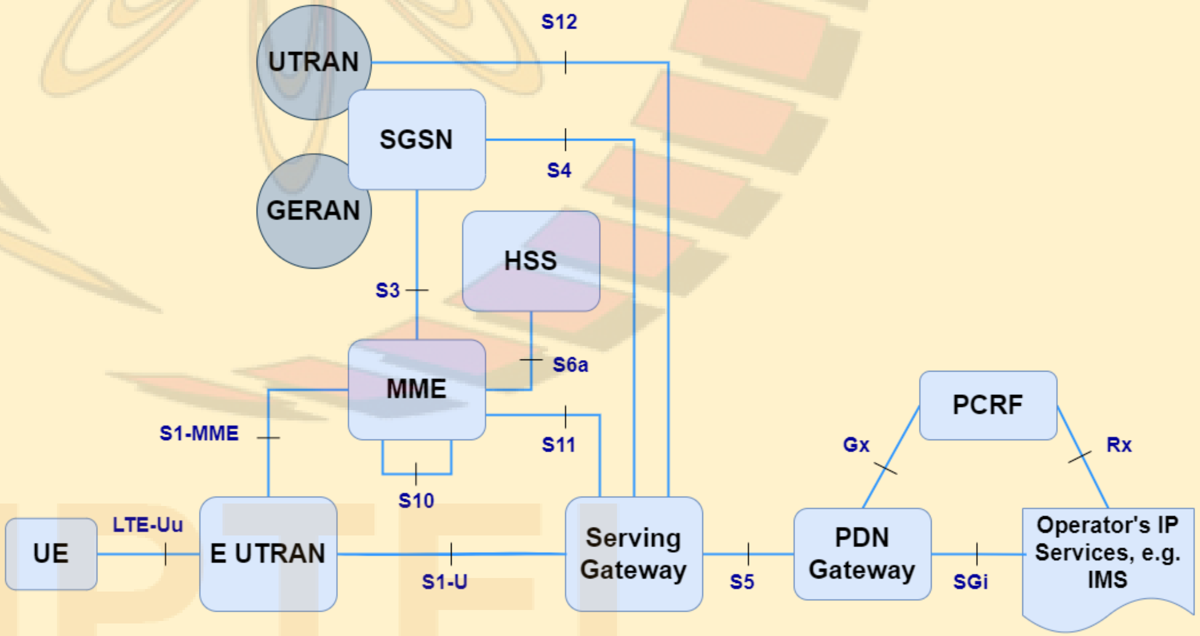
Overview of 3G Architecture (contd.)

- In the CN, the most important element in the CS domain is the switching element MSC:
  - ❑ typically integrated with a Visitor Location Register (VLR) that contains a database of the users currently in the location area controlled by the MSC
  - ❑ the Gateway Mobile Switching Centre (GMSC) takes care of connections to the Public Switched Telephone Network (PSTN)
- In the PS domain:
  - ❑ the role of MSC/VLR is taken by the SGSN, while the GGSN takes care of connecting to the Internet
- Static subscriber information is maintained in the Home Location Register (HLR)
  - ❑ typically integrated with the Authentication Centre (AuC) that maintains the permanent security information related to subscribers



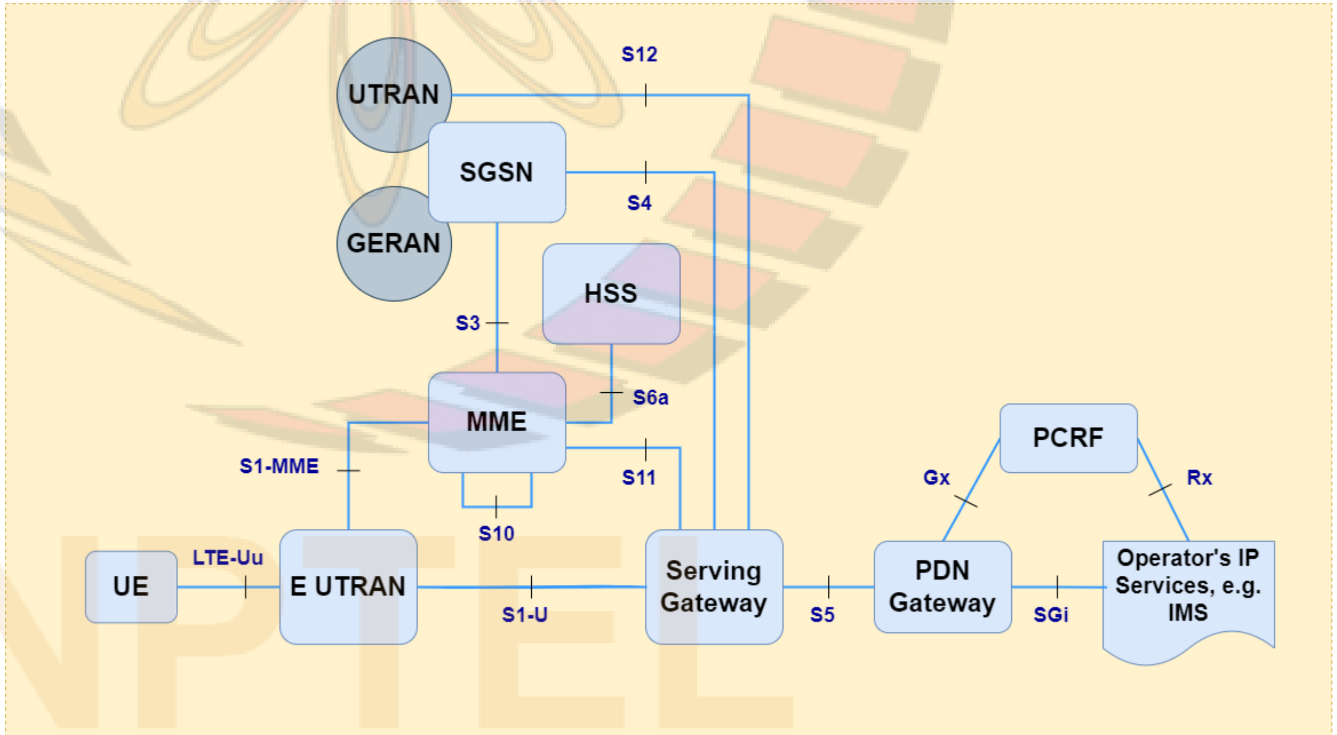
EPS

- Goals of the EPS are:
  - ❑ higher data rates,
  - ❑ lower latency,
  - ❑ high level of security,
  - ❑ enhanced quality of service (QoS),
  - ❑ capabilities for interworking with legacy systems
- Main means to achieve these goals are:
  - ❑ the new radio interface and the new RAN based on it (E-UTRAN) and
  - ❑ a flat IP-based architecture that has only two network elements on the user plane (evolved NodeB (eNB) and Serving Gateway (S-GW))
- Fig. illustrates EPS network architecture in a case where the UE is not roaming into a different network than where it has its subscription
  - ❑Note: the legacy RANs UTRAN and GERAN are included in the system together with the legacy CN element SGSN



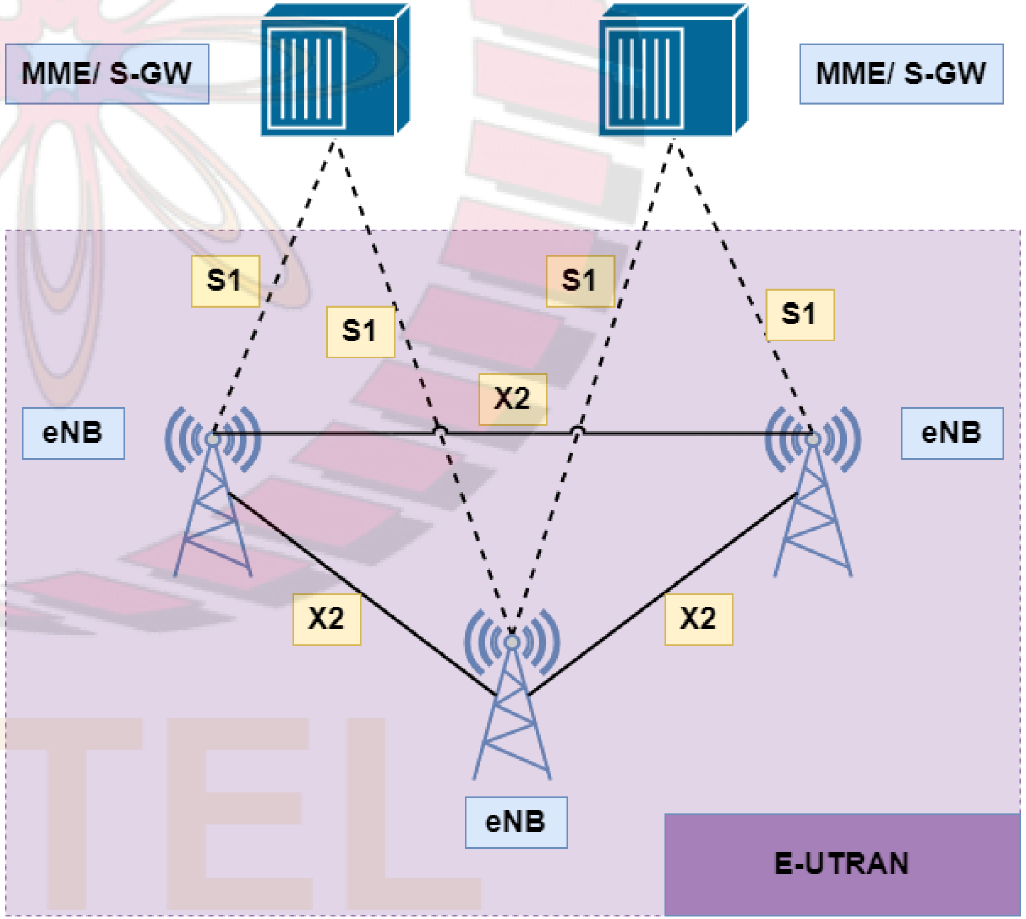
EPS (contd.)

- In EPS, there is a new CN element called Mobility Management Entity (MME)
- HLR of the original GSM and 3G architecture is extended to the Home Subscriber Server (HSS)
- CN element for user plane handling is called Serving Gateway
- Packet Data Network Gateway (PDN GW) handles the traffic towards PDNs
- CN of the EPS is called Evolved Packet Core (EPC)



E-UTRAN Architecture

- Architecture of E-UTRAN depicted in fig.
- eNB is the only type of network element in E-UTRAN
- There is an interface between two eNBs, which facilitates fast handovers between different BSs


MME/ S-GW
MME/ S-GW
S1
S1
S1
S1
X2
eNB
eNB
X2
X2
eNB
E-UTRAN