SWINBURNE UNIVERSITY OF TECHNOLOGY

NSR/AS

Cellular Network Security

Lecture Twenty-seven

Outline of Lecture

- Cellular overview
- Cellular generations
- Security in 2G, 3G and 4G networks

Cellular Networks

- Sometimes “Personal Communications Systems”
- Owned and operated by Telecommunications Companies
- Wide coverage, large number of users (subscribers)
- Users are mobile
  - Variable traffic loads
  - Handover between “Base Stations”
- Expensive to deploy and run

Cellular Networks

- A cellular radio network consists of a large number of low power base stations, each having limited coverage area called a **cell**.
  - Low power means up to about 60 Watts
  - Maximum distance differs between generation but maximum about 35 km (but smaller for later generations)
- Radio channels are allocated to each cell so as to minimize interference, provide adequate performance and cater to the traffic loads in the area.
- Nearby cells are allocated different groups of channels so as to reduce interference.
- Network has to **handover** mobile stations between cells

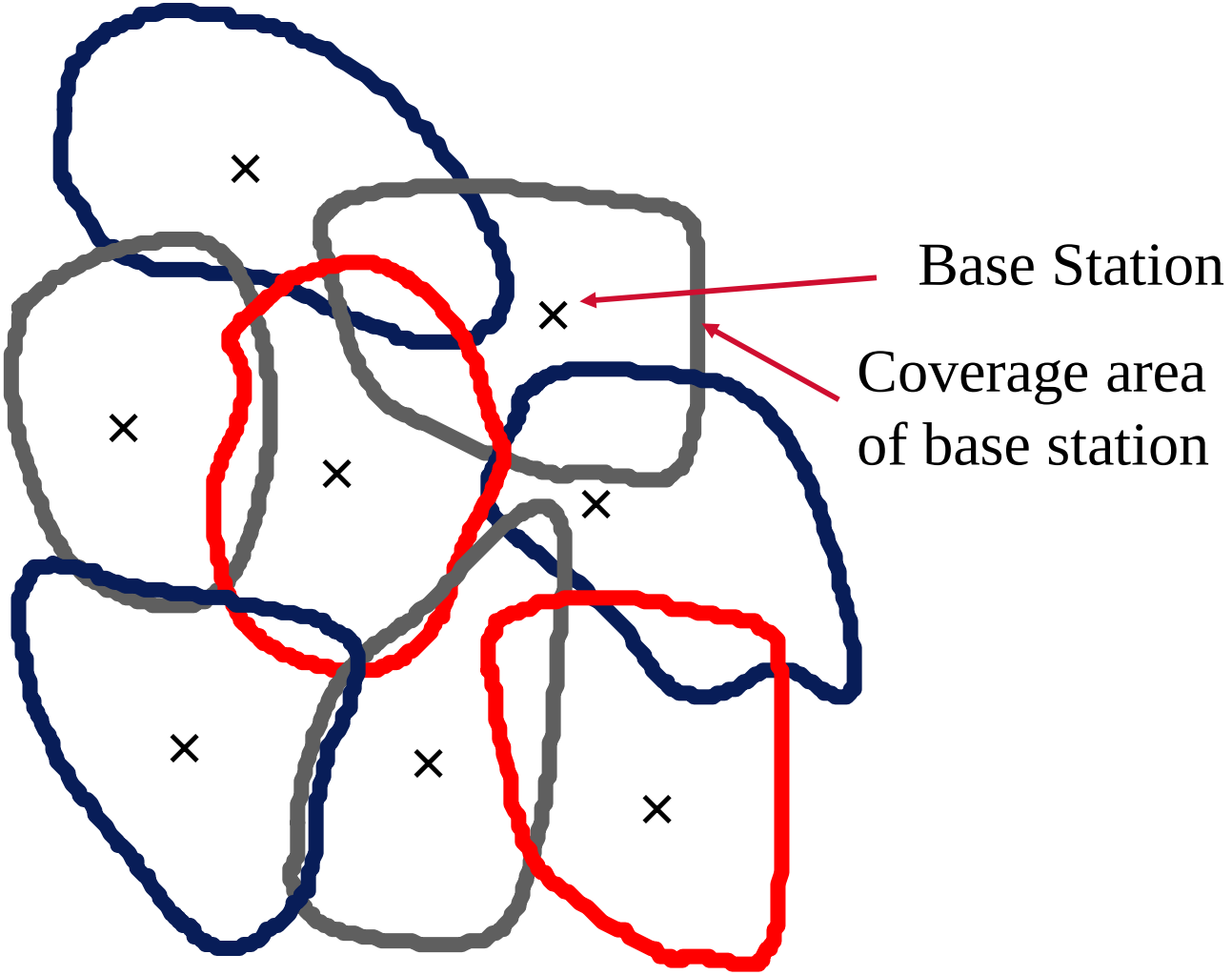
Cellular network security issues

- Wireless is inherently insecure
  - Cannot (easily) constrain a wireless signal to confined space
- Users are mobile
  - Mobility introduces many new components into a network all of which are susceptible to attack
    - base stations, access points
  - Handset or laptops can be stolen
- Bandwidth is constrained
  - Security protocols such as IPSec impose additional layers of encapsulation which result in additional overhead traffic
- Handsets are resource constrained
  - Limited in computing power (for encryption) and battery power

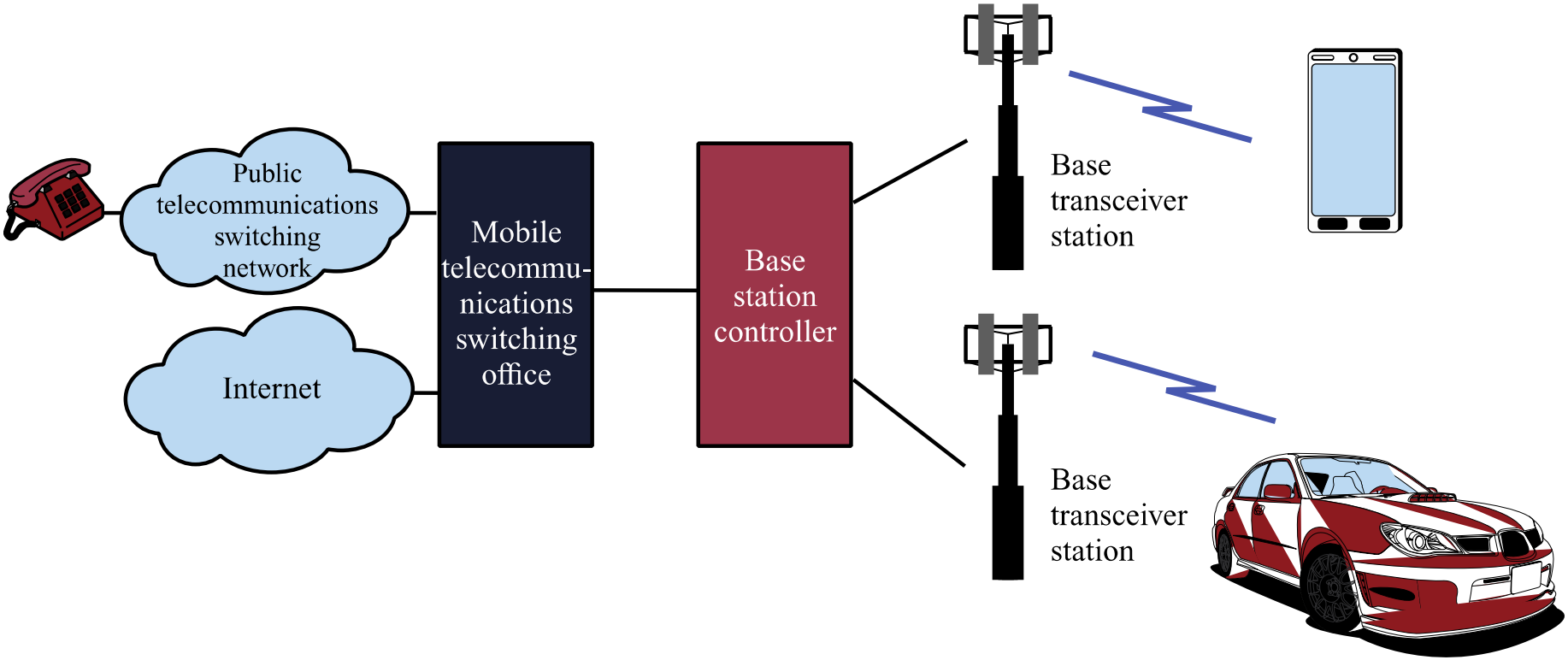
Security consequences for wireless

- Mobile phones and wireless PDAs are consumer items
  - Need to limit the cost and effort needed to make them secure if they are to be affordable
- Telephone companies may have hundreds of thousands of customers
  - Systems and procedures have to be automated and fool-proof
- Mobile phone call records are often used in legal cases
  - Billing information has to be reliable and retained

Cellular Coverage



Architecture of cellular network



From Beard and Stallings "Wireless Communications Networks and Systems", 2016

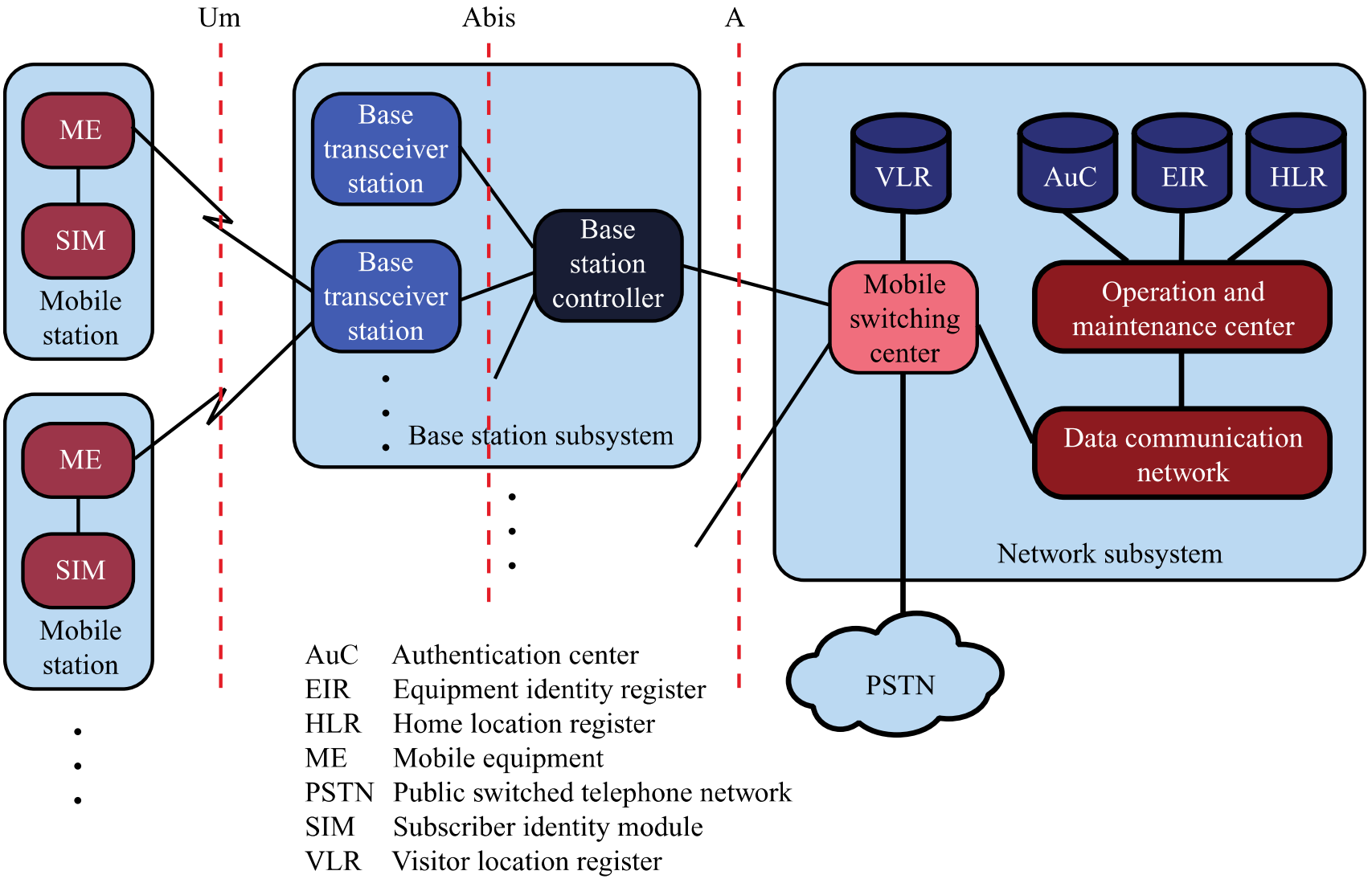
Cellular Systems Terms

- Base Station (BS) – includes an antenna, a controller, and a number of receivers
- Mobile telecommunications switching office (MTSO) – connects calls between mobile units
- Two types of channels available between mobile unit and BS
  - Control channels – used to exchange information having to do with setting up and maintaining calls
  - Traffic channels – carry voice or data connection between users

History of Cellular Networks

Generation	Characteristics	Dominant Technology
1G	Analog, Circuit Switched, FDM, No security	AMPS
2G	Digital, Circuit Switched, TDMA or CDMA, SIM card, Symmetric key cryptography, Challenge response authentication	GSM
3G	Circuit and Packet Switched, CDMA, Symmetric key cryptography, multiple algorithms	UMTS
4G	Packet Switched, OFDMA, Simplified core, Symmetric key cryptography, multiple algorithms	LTE
5G	Packet Switched, OFDMA, Many small cells, high frequencies, Crypto based on 4G but able to support non 5G authentication	5G NR

2G GSM



AuC Authentication center
EIR Equipment identity register
HLR Home location register
ME Mobile equipment
PSTN Public switched telephone network
SIM Subscriber identity module
VLR Visitor location register

Mobile Station (MS)

- Mobile Station provides the user interface and the air interface to the BSS
- User interface
  - Microphone, speaker, keypad, display, cable interface for other devices
- Air interface
  - Radio modem and an antenna
- Two nodes
  - Mobile Equipment
    - Handset
  - Subscriber Identity Module
    - SIM Card

Subscriber Identity Module (SIM)

- Smart card
- Specifies address and type of service
- Stores SMS messages
- Stores information about user and configuration
  - Protected by a PIN
- Stores encryption algorithms and keys

Base Station Subsystem (BSS)

- BSS consists of base station controller and one or more base transceiver stations (BTS)
- Each BTS defines a single cell
  - Includes radio antenna, radio transceiver and a link to a base station controller (BSC)
- BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within BSS, and controls paging

Network Subsystem (NS)

- NS provides link between cellular network and public switched telecommunications networks
  - Controls handoffs between cells in different BSSs
  - Authenticates users and validates accounts
  - Enables worldwide roaming of mobile users
- Central element of NS is the mobile switching center (MSC)

Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to it
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

Identification in GSM

- Three identifiers associated with every user / handset
- MSISDN
  - directory phone number
- IMEI
  - International Mobile International Equipment Identifier
  - Associated with the handset equipment itself
- IMSI
  - International Mobile Subscriber Identifier
    - SIM Card number

Authentication of Handset / SIM to the Network

- Based on the Subscriber Identity Module (SIM) card
  - Multifactor authentication
    - PIN number
    - SIM card is a token
- SIM card contains information about the account, not the handset
  - Depending on handset restrictions it is possible to move a SIM card from one handsets to another but still use the same account

SIM Card

- SIM card contains
  - International Mobile Security Identifier (IMSI)
  - SMS messages
  - Secret key Ki
  - Encryption and authentication algorithms
- Knowledge of Ki (by the handset) is sufficient proof of identity to the network

Secret key Ki

- GSM uses secret, symmetric key cryptography
  - GSM predates public key cryptography
- Secret key is referred to as Ki in the GSM specification
- Ki is Created at the time the account is opened
- Written onto the SIM card and into the HLR
  - Encrypted on the SIM card
  - Ki is never transmitted across the air interface
  - Manual key distribution

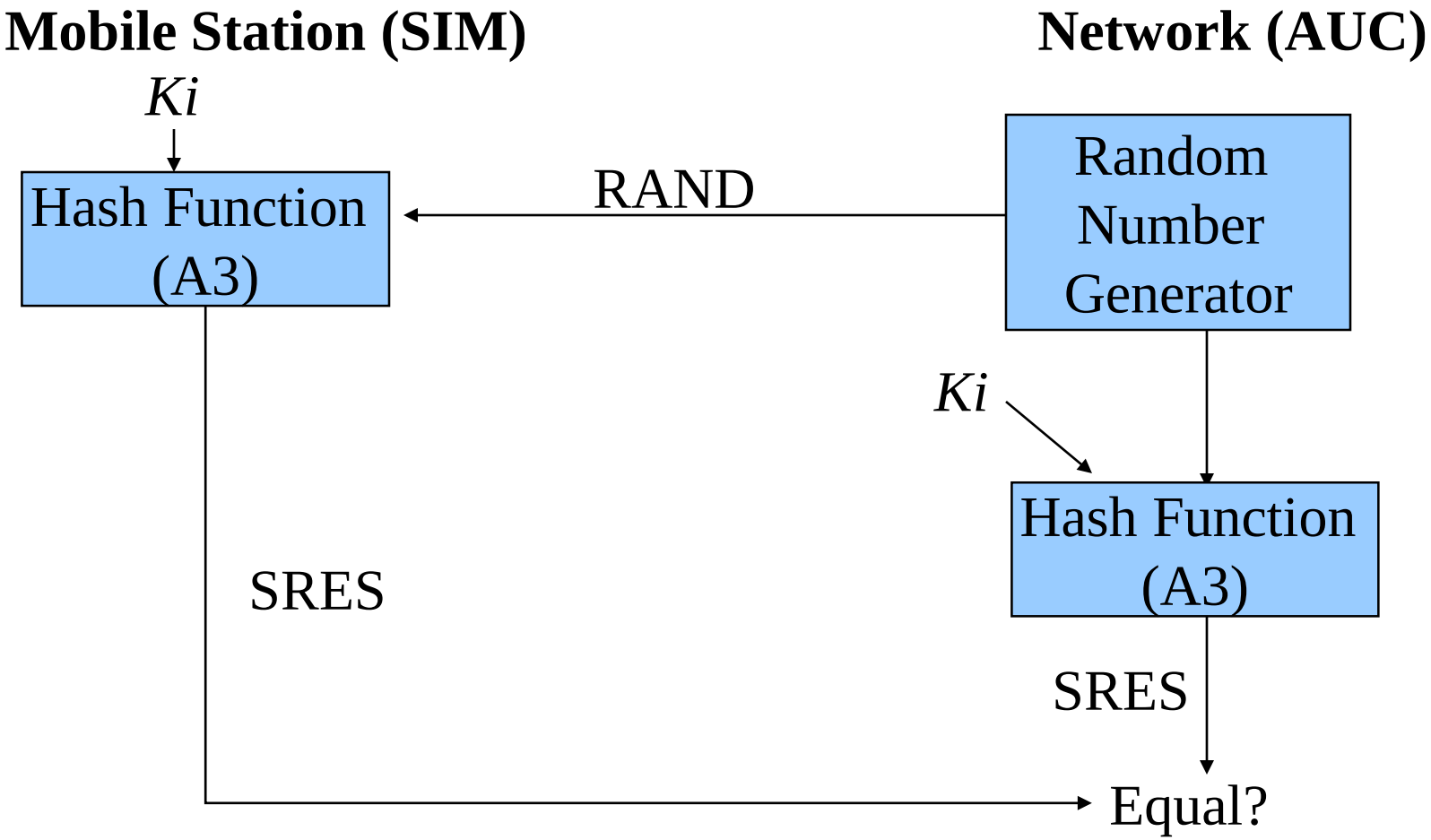
GSM encryption and authentication

- The GSM standard uses three cryptographic algorithms for encryption and authentication
  - Denoted by A3, A5 and A8
- The standard does not specify A3 or A8
  - Used in authentication and generation of a session key
- But it does say there must be such algorithms
  - Provides sample implementations
- A3 is used for authentication
- A8 is used for generation of a session key
- A5 used for encryption
- There is no A1, A2, A4 etc

Authentication of SIM card to Network

- A simple Challenge Authentication Protocol
- Uses algorithm A3 defined by the operator, and the secret key Ki stored on the SIM card
- Network issues the handset with a challenge
  - A random 128 bit number denoted by RAND
  - The handset uses the A3 algorithm and Ki to encrypt RAND to produce the result SRES (short for Signed RESult)
  - SRES is transmitted, in the clear, back to the AUC where the same procedure using Ki has been carried out
  - If the SRES values agree the user is authenticated

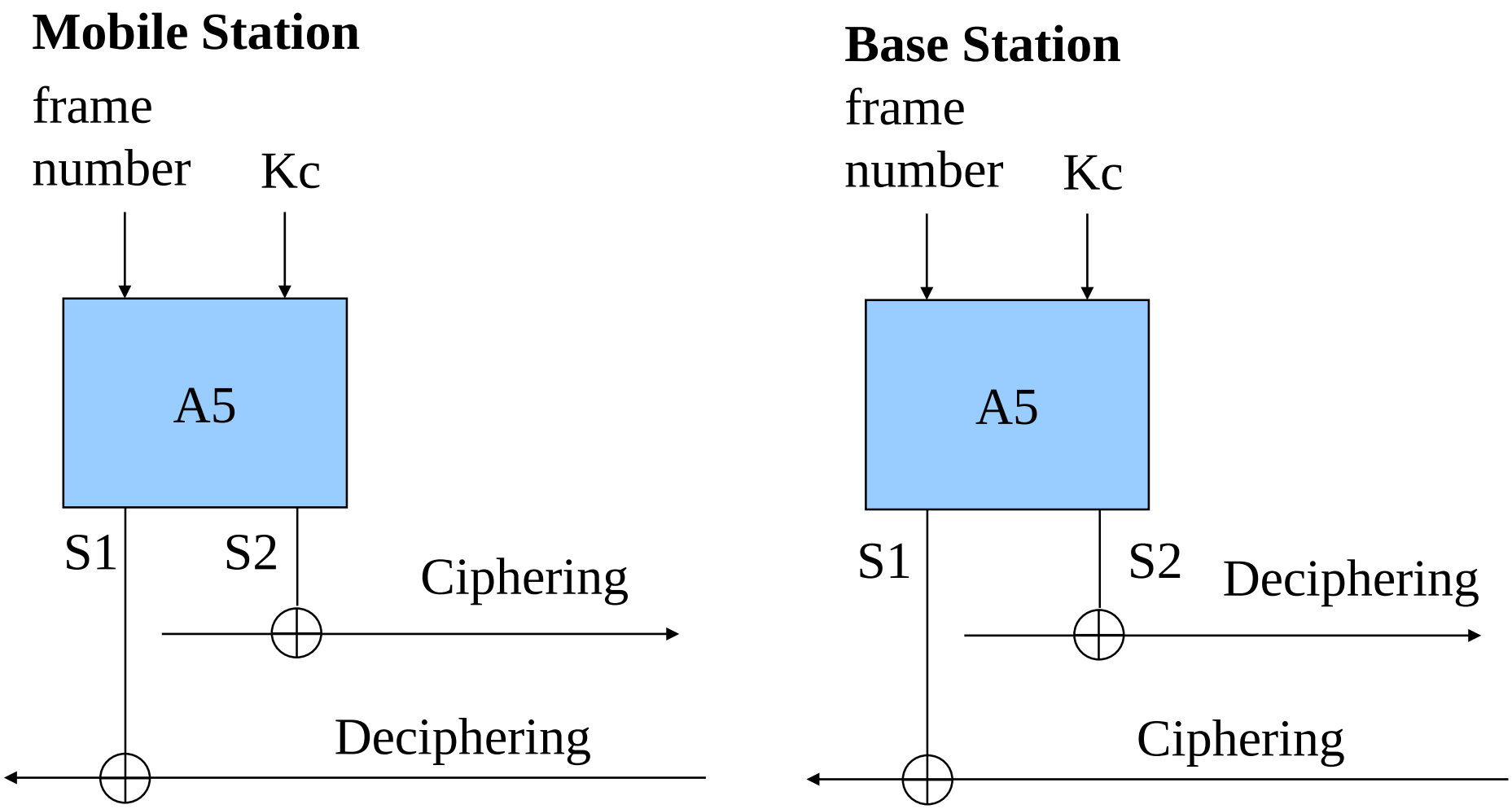
Authentication



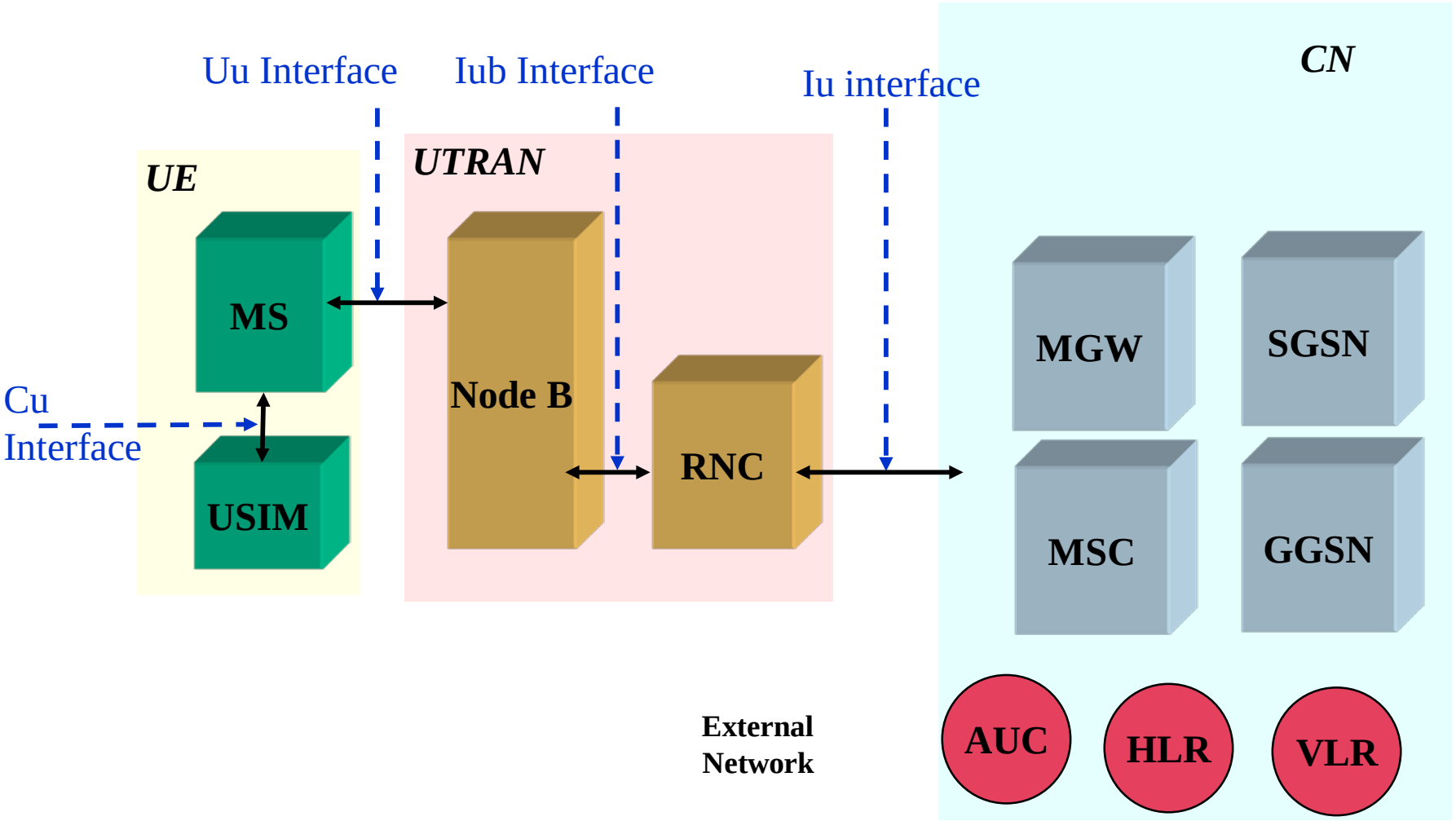
Encryption in GSM

- GSM uses a session key Kc
  - Ki is never used directly in encrypting messages
  - A session key Kc is used for encrypting messages
  - The RAND value used in authentication is also used to create a ciphering key Kc
  - Kc is produced by the A8 algorithm using Ki and RAND as inputs
- Encryption uses Kc and the A5 algorithm
  - For each frame A5 generates two 114 bit sequences (S1 and S2)
    - inputs are the frame number and Kc
  - Encryption is carried out with S1 and Decryption with S2
  - Each S1 and S2 sequence is then XOR ed with the data sequence

A5 operation



3G UMTS Network Elements



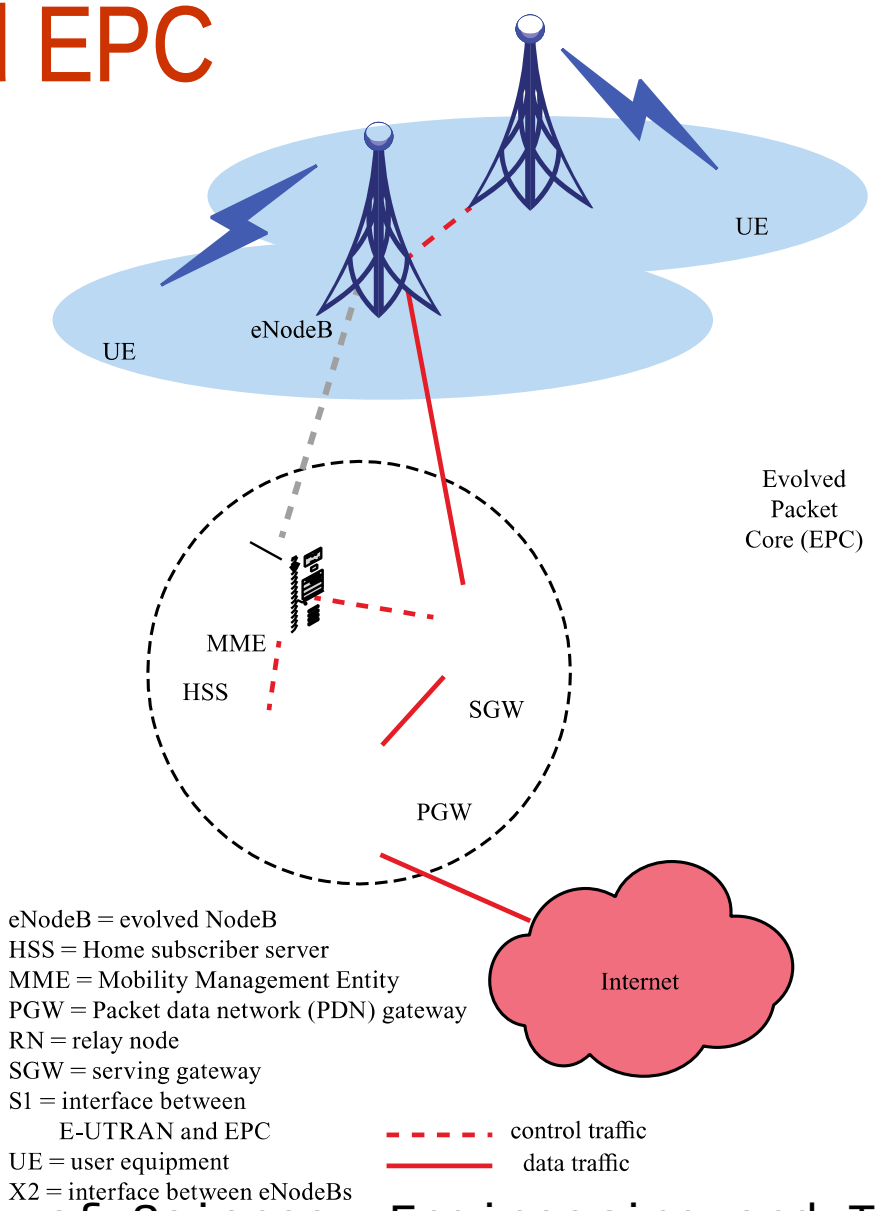
UMTS Security

- Builds on GSM security
- Corrects problems with GSM Security
- Additional security features

UMTS Additional security features

- Two way authentication
  - User can authenticate identify of network
- Stronger algorithms and longer keys
- Integrity mechanisms to defend against replay
- Encryption can be extended beyond radio interface
- Notification that encryption is on or off
- Additional user flexibility as to security features selected
- Backwards compatible with GSM

4G LTE and EPC



4G

- Requirements
  - IP core
  - Separate mobility management
  - Heterogeneous radio network interfaces
  - Heterogeneous handoff (handover)
- In Australia 4G technology is LTE-Advanced
  - Strong industry backing
  - Satisfies the above requirements

LTE / SAE

- Long Term Evolution (of radio networks)
- Up to 100 Mbps in a cellular architecture
- An all IP core
  - System Architecture Evolution (SAE)
- Simplified architecture (when compared with 3G / UMTS)

LTE Security

- Similar capabilities to 3G
- Major difference is need to interwork with other networks
  - 3G, 2G, WLAN, WiMax
- IPSec (optional) in the network core
- Two sets of cryptographic algorithms in all implementations
  - If one breaks, still have the other one
  - AES and SNOW 3G (a stream cipher with 128 or 256 bit keys)
  - Third cryptographic algorithm being developed

Conclusion

- Overview of cellular networks
- Security of 2G, 3G, 4G networks