Mobile and Sensor Systems

Lecture 2: Mobile Medium Access Control Layer and Telecommunications

Dr. Cecilia Mascolo

UNIVERSITY OF CAMBRIDGE

In this Lecture

- In this lecture we will discuss aspects related to the MAC Layer of wireless networks
  - In comparison with wired networks
  - In terms of how multiplexing in applied
  - In terms of carrier sensing
- We will also describe the architecture of telecommunication networks

UNIVERSITY OF CAMBRIDGE

Access methods SDMA/FDMA/TDMA

- SDMA (Space Division Multiple Access)
  - segment space into sectors, use directed antennas
  - cell structure
- FDMA (Frequency Division Multiple Access)
  - assign a certain frequency to a transmission channel between a sender and a receiver
  - permanent (e.g., radio broadcast), slow hopping (e.g., GSM), fast hopping (FHSS, Frequency Hopping Spread Spectrum)
- TDMA (Time Division Multiple Access)
  - assign the fixed sending frequency to a transmission channel between a sender and a receiver for a certain amount of time
- The multiplexing schemes presented in the previous lecture are now used to control medium access!

UNIVERSITY OF CAMBRIDGE

Access method CDMA

- CDMA (Code Division Multiple Access)
  - all terminals send on the same frequency roughly at the same time and can use the whole bandwidth of the transmission channel
  - each sender has a unique random number, the sender XORs the signal with this random number
  - the receiver can “tune” into this signal if it knows the random number, tuning is done via a correlation function
- Disadvantages:
  - higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
  - all signals should have the same strength at a receiver
- Advantages:
  - all terminals can use the same frequency, no planning needed
  - huge code space compared to frequency space

UNIVERSITY OF CAMBRIDGE

Comparisons

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

Limitations of multiplexing

- Multiplexing is one way to allow a basic share of medium to be shared more efficiently through the definition of “channels”
- Once channels are established packets will be sent through that
  - Might be a bit rigid as a method
  - For example, frequency division multiplexing would have issues with large numbers of users.
  - Also depending on traffic and time some users might want to send more or less
- More ad hoc approaches exist which allow channels to be shared in a “statistical” way

Review: Ethernet Medium Access Control (MAC)

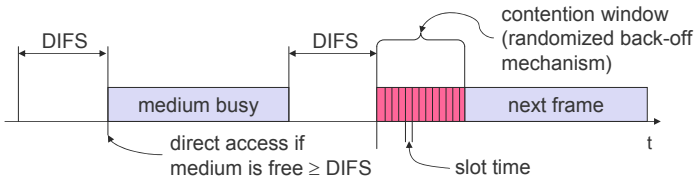
- In Ethernet based fixed networks where you have wires between computers:
- CS (Carrier Sense): listen for others’ transmissions before transmitting; defer to others you hear
- CD (Collision Detection): as you transmit, listen and verify you hear exactly what you send; if not, back off random interval, within exponentially longer range each time you transmit unsuccessfully

Can CD be applied on wireless networks?

Can we apply the same MAC protocols in wireless?

- Problems in wireless networks
  - signal strength decreases proportionally to the square of the distance
  - the sender would apply CS and CD, but collisions happen at the receiver
  - it might be the case that a sender cannot “hear” the collision, i.e., CD does not work
  - furthermore, CS might not work if, e.g., a terminal is “hidden”

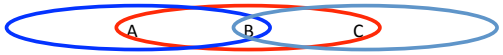
CSMA/CA: Carrier Sensing Multiple Access Protocol with Collision Avoidance



• CSMA/CA: sense medium. If free transmit (although this might generate collision at the receiver). If not, wait with a back off strategy. Transmit when medium is sensed free.

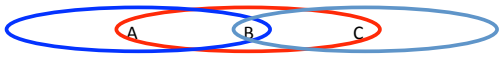
Hidden Terminal

- Hidden terminals
  - A sends to B, C cannot receive from A
  - C wants to send to B, C senses a "free" medium (CS fails)
  - Collision at B, A cannot receive the collision (CD fails)
  - A is "hidden" for C



Exposed Terminal

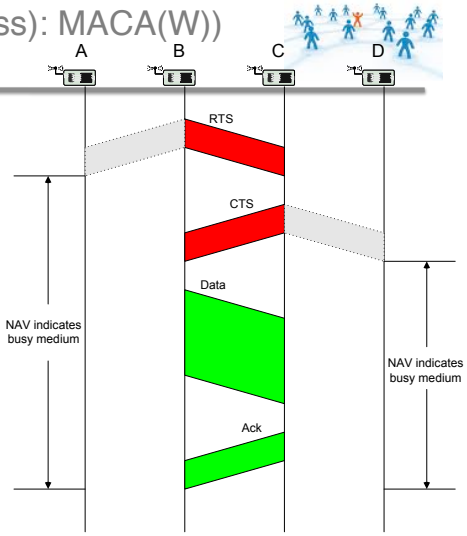
- Exposed terminals
  - B sends to A, C wants to send to another terminal (not A or B)
  - C has to wait, CS signals a medium in use
  - but A is outside the radio range of C, therefore waiting is not necessary
  - C is "exposed" to B



Multiple Access with Collision Avoidance (for Wireless): MACA(W))

- Sender B asks receiver C whether C is able to receive a transmission ***Request to Send (RTS)***
- Receiver C agrees, sends out a ***Clear to Send*** (***CTS***)
- Potential interferers overhear either RTS or CTS and know about impending transmission and for how long it will last
  - Store this information in a ***Network Allocation Vector***
- B sends, C acks

! ***MACA(W) protocol*** (used e.g. in ***IEEE 802.11***)



MACA(W)

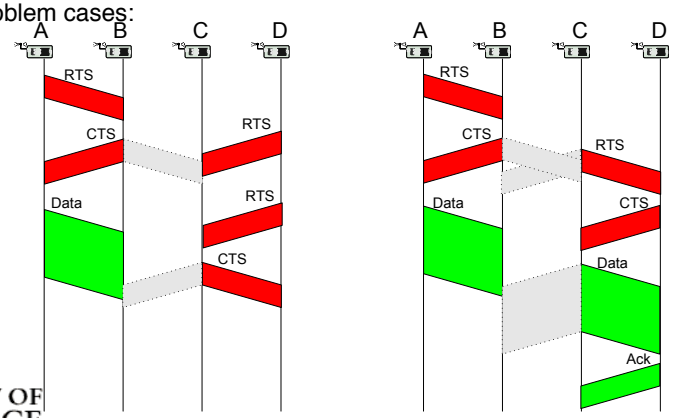
- Absent CTS, sender backs off exponentially before retrying
- RTS and CTS can still themselves collide at their receivers; less chance as they're short;

- **What's the effect on exposed terminal problem?**

UNIVERSITY OF CAMBRIDGE

RTS/CTS

- RTS/CTS ameliorate, but do not solve hidden/exposed terminal problems
- Example problem cases:



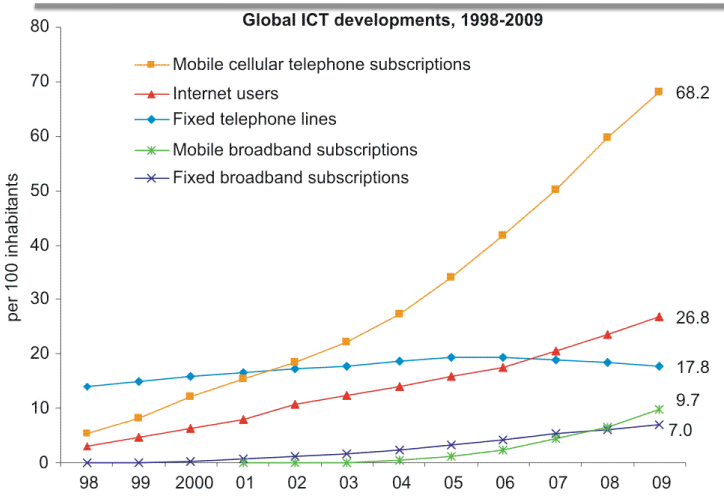
UNIVERSITY OF CAMBRIDGE

The 802.11 Protocol

- 802.11 uses 2 modes of operation: a basic CSMA/CA (in base station mode) and the RTS/CTS mode.
- Generally 802.11 drivers leave the RTS/CTS off by default.
- Also tests in practice show that hidden terminal might not be a problem in most cases as interference range is more than double communication range. Consider A->B<-C when A transmits it is very likely C can sense A's carrier directly.

UNIVERSITY OF CAMBRIDGE

Mobile Phone Subscribers



Source: ITU World Telecommunication/ICT Indicators database.

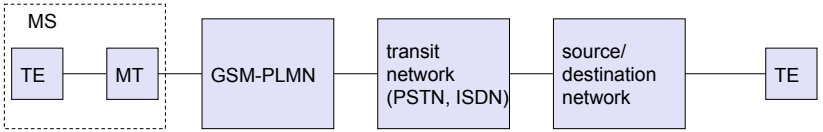
Telecomms Stats & GSM

- July 2010 (gsmworld.com): The GSMA announced that the number of global mobile connections has surpassed the 5 billion mark, according to new data from mobile industry analysis firm Wireless Intelligence. The achievement comes just 18 months after the 4 billion connection milestone was reached at the end of 2008, and Wireless Intelligence is predicting that the mobile industry will reach 6 billion global connections in the first half of 2012.

- GSM
  - formerly: Groupe Spéciale Mobile (founded 1982)
  - now: Global System for Mobile Communication
- Today many providers all over the world use GSM (219 countries in Asia, Africa, Europe, Australia, America)
  - more than 75% of all digital mobile phones use GSM

GSM: Mobile Services

- GSM offers
  - several types of connections
    - voice connections, data connections, short message service
    - multi-service options (combination of basic services)
- Three service domains
  - Bearer Services
  - Telematic Services
  - Supplementary Services (not discussed)



Bearer Services

- Telecommunication services to transfer **data**
  - This service is the one which needed to change most given the importance that data transfer is acquiring
- Specification of services up to the terminal interface (OSI layers 1-3)

- Original standard:
  - data service (circuit switched or packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s
  - Low rates assuming data is a small proportion of the traffic!!

- Today: data rates of approx. 50 kbit/s possible, given the importance of data transmission

Tele Services I

- Telecommunication services enable **voice** communication on mobile phones
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
  - mobile telephony
    primary goal of GSM was to enable mobile telephony offering the traditional analog bandwidth of 3.1 kHz
  - Emergency number
    common number throughout Europe; mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)

Tele Services II

- Additional services
  - Non-Voice-Teleservices
    - group 3 fax
    - voice mailbox (implemented in the fixed network supporting the mobile terminals)
    - electronic mail (MHS, Message Handling System, implemented in the fixed network)
    - …
    - **Short Message Service (SMS)**
      alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS
      (**almost ignored in the beginning now the most successful add-on!**: *note that it does not use the data service but the voice channels*)

UNIVERSITY OF CAMBRIDGE

Ingredients 1: Mobile Phone

The visible but smallest part of the network!

UNIVERSITY OF CAMBRIDGE

Ingredients 2: Antennas

Still visible – cause many discussions…

UNIVERSITY OF CAMBRIDGE

Ingredients 3: Infrastructure 1

Base Stations

Cabling

Microwave links

UNIVERSITY OF CAMBRIDGE

Ingredients 3: Infrastructure 2

Switching units

Management

Data bases

Not „visible“, but comprise the major part of the network (also from an investment point of view…)

Monitoring

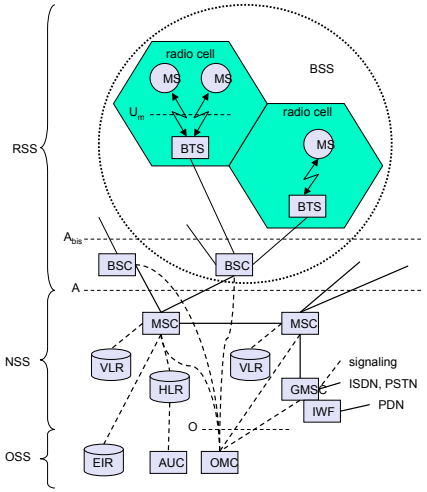
UNIVERSITY OF CAMBRIDGE

Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

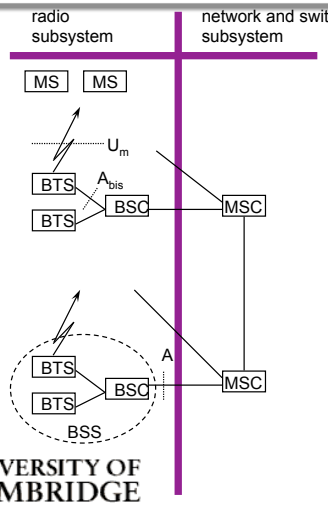
UNIVERSITY OF CAMBRIDGE

GSM: elements and interfaces



UNIVERSITY OF CAMBRIDGE

System architecture: radio subsystem



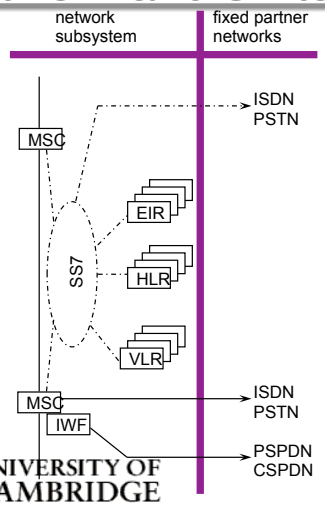
- Components
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- Interfaces
  - U_m : radio interface
  - A_{bis} : standardized, open interface with 16-64 kbit/s user channels
  - *A*: standardized, open interface with 64 kbit/s user channels

UNIVERSITY OF CAMBRIDGE

Radio subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
  - Mobile Stations (MS)

System architecture: network and switching subsystem



- Components
  - MSC (Mobile Services Switching Center):
  - IWF (Interworking Functions)
  - ISDN (Integrated Services Digital Network)
  - PSTN (Public Switched Telephone Network)
  - PSPDN (Packet Switched Public Data Net.)
  - CSPDN (Circuit Switched Public Data Net.)
- Databases
  - HLR (Home Location Register)
  - VLR (Visitor Location Register)
  - EIR (Equipment Identity Register)
- SS7: covers routing within the network and connectivity

Network and switching subsystem

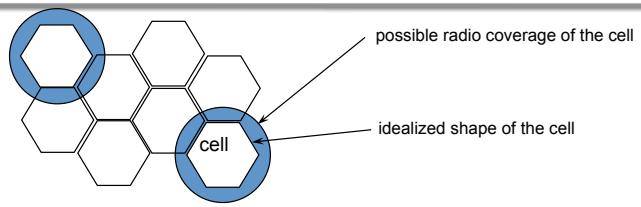
- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - Mobile Services Switching Center (MSC)
    controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)
      central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)
      dynamic and local database for a subset of user data, including data about all user currently in the domain of the VLR. VLRs avoid continuous access to HLR

Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

GSM: cellular network

segmentation of the area into cells



- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells handover of the connection to the neighbor cell

UNIVERSITY OF CAMBRIDGE

Base Transceiver Station and Base Station Controller

- Tasks of a BSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

UNIVERSITY OF CAMBRIDGE

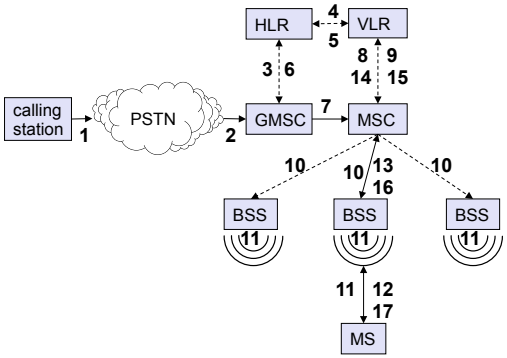
Storing Information of Users

- The Home location register (HLR) stores the mobile ISDN number, international subscriber identity but also location area (LA) and the mobile subscriber roaming number (MSRN), the current VLR and MSC.
- Information is updated when user leaves the LA
- The Visitor location register (VLR) is associated to each MSC and is dynamic: stores same info as HLR copying it from HLR as soon as a users comes into the LA. It avoids frequent access to HLR.

UNIVERSITY OF CAMBRIDGE

Mobile Terminated Call

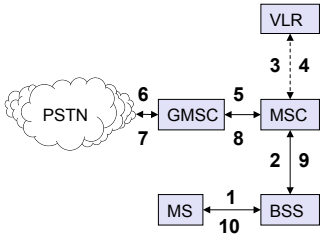
- 1: calling a GSM subscriber
- 2: forwarding call to Gateway MSC
- 3: signal call setup to HLR
- 4, 5: request MSRN (mobile station roaming number) from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection



UNIVERSITY OF CAMBRIDGE

Mobile Originated Call

- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call

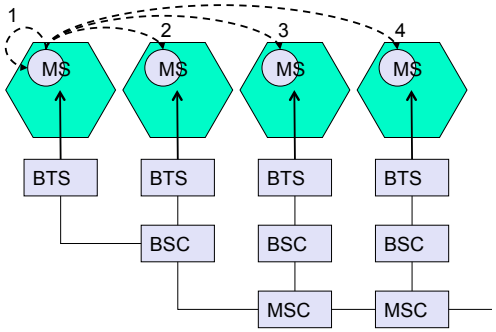


UNIVERSITY OF CAMBRIDGE

4 types of handover

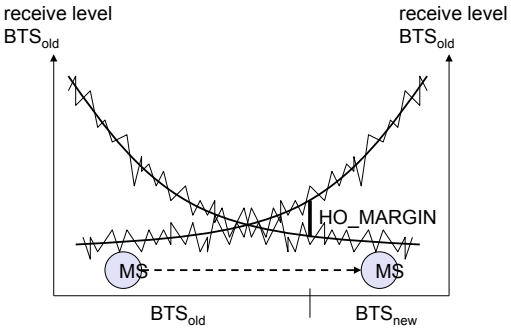
There are 4 types of handover:

- Change of frequency due to interference inside a cell
- Handover between BTSs
- Handover between BSCs (described later)
- Handover between MSCs



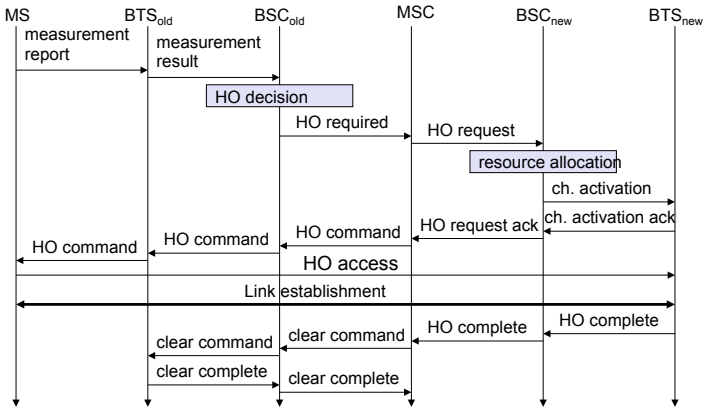
UNIVERSITY OF CAMBRIDGE

Handover decision



UNIVERSITY OF CAMBRIDGE

Handover procedure



UNIVERSITY OF CAMBRIDGE

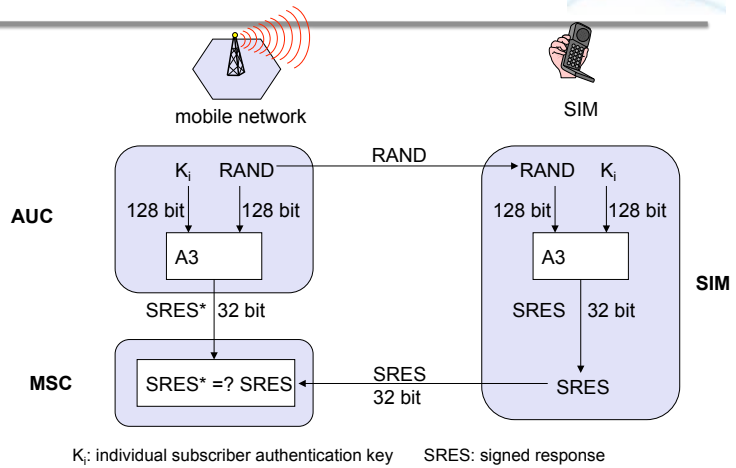
Security in GSM

- Security services
  - access control/authentication
    - user → SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM → network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - Only VLR assigned user temporary identifiers TMSI (Temporary Mobile Subscriber Identity) are used
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

UNIVERSITY OF CAMBRIDGE

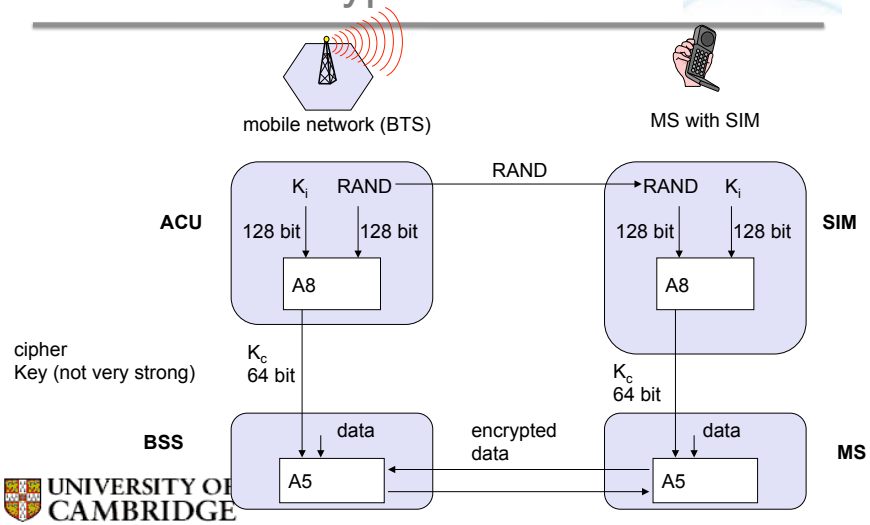
GSM - authentication



K_i: individual subscriber authentication key SRES: signed response

UNIVERSITY OF CAMBRIDGE

GSM - key generation and encryption



UNIVERSITY OF CAMBRIDGE

Summary

- We have shown how multiplexing can be used at the MAC layer
- We have explained the limits of carrier sensing
- We have described the problems related to "hidden and exposed" terminals
- We have described the basic principles and architecture of a telecommunication system and given the concrete example of GSM

UNIVERSITY OF CAMBRIDGE