Sécurité des Réseaux, Master CSI 2

J.Bétréma, LaBRI, Université Bordeaux 1

Communications sans fil

Bandes de fréquences

Source:

Andy Dornan

The Essential Guide to Wireless Communications Applications

Prentice Hall

Panorama

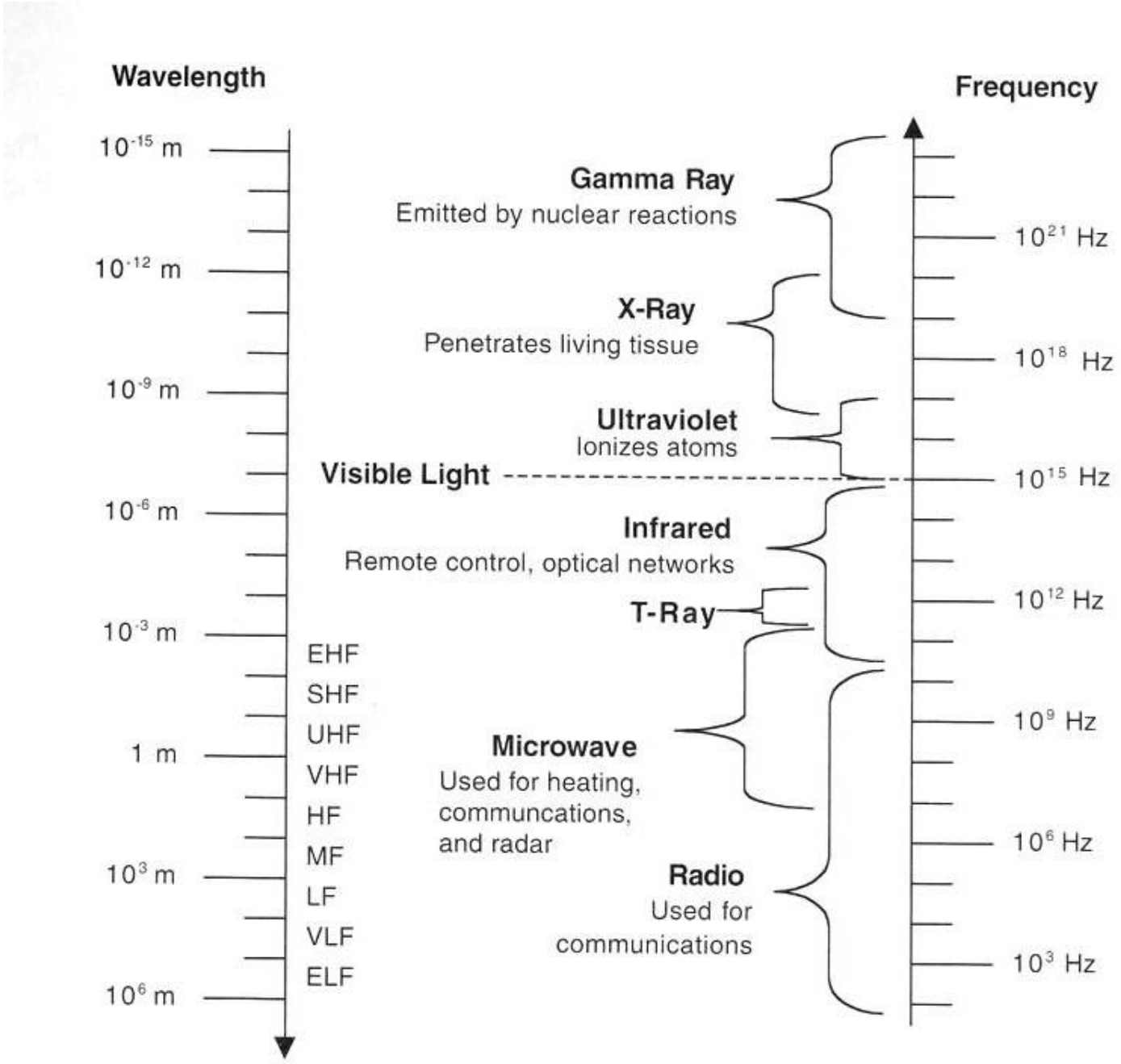


Figure 2.2
The electromagnetic spectrum.

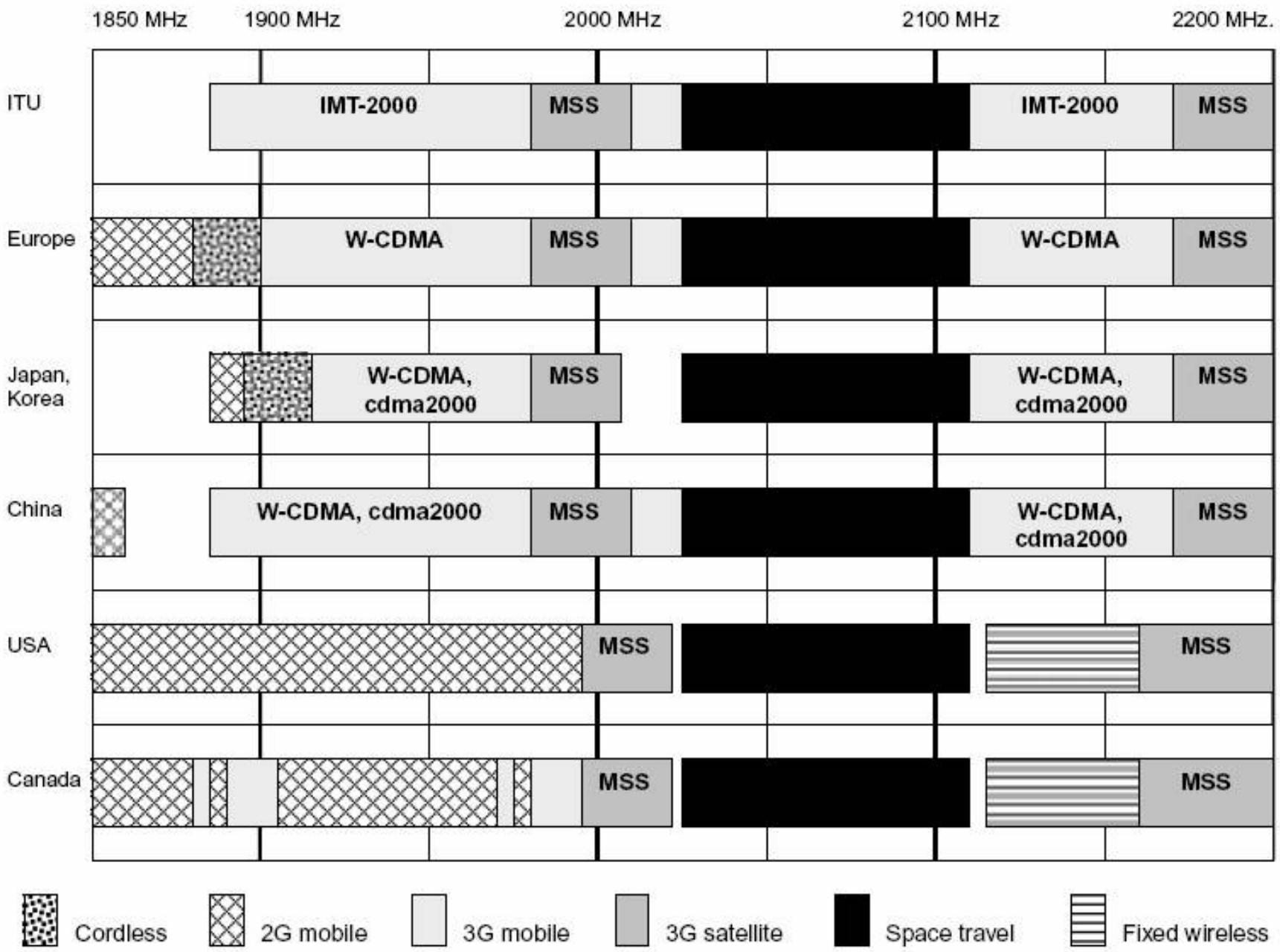
Ondes radios

Longueur d'onde	Fréquence	Nom	Usage
1-10 mètres	30-300 MHz	**VHF**: Very High Frequency	Radio FM Télévision
0.1-1 mètre	300 MHz-3 GHz	**UHF**: Ultra High Frequency	Télévision Téléphonie mobile Réseaux sans fil
10-100 mm	3-30 GHz	**SHF**: Super High Frequency	Satellites
1-10 mm	30-300 GHz	**EHF**: Extra High Frequency	Satellites Radars

Spectre alloué à la téléphonie 3G

- ITU: International Telecommunications Union
- IMT-2000: International Mobile Telecommunications
- UMTS: Universal Mobile Telecommunications System (standard W-CDMA européen)
- W-CDMA: Wideband Code Division Multiple Access
- MSS: Mobile Satellite System
- Cordless: téléphone sans fil (• mobile, cellulaire)

Spectre 3G (2)


1850 MHz
1900 MHz
2000 MHz
2100 MHz
2200 MHz.
ITU
IMT-2000
MSS
IMT-2000
MSS
Europe
W-CDMA
MSS
W-CDMA
MSS
Japan, Korea
W-CDMA, cdma2000
MSS
W-CDMA, cdma2000
MSS
China
W-CDMA, cdma2000
MSS
W-CDMA, cdma2000
MSS
USA
MSS
MSS
Canada
MSS
MSS
Cordless
2G mobile
3G mobile
3G satellite
Space travel
Fixed wireless

ISM

Industrial, Scientific and Medical: 2.4-2.5 GHz

- Wi-Fi (802.11) et Bluetooth
- Fours à micro-ondes, etc.

Pas de licences.$\Rightarrow$ compétition

GSM

Combine:

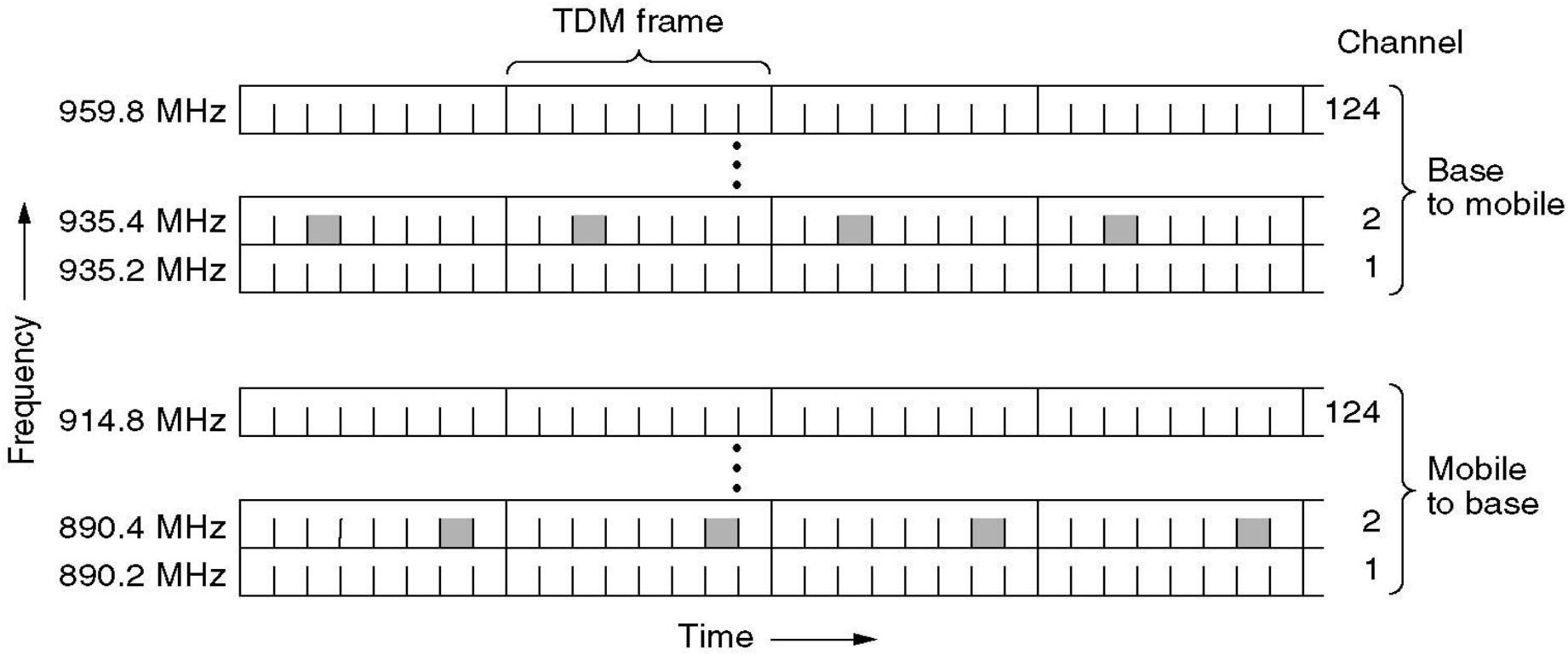
- FDMA : multiplexage fréquentiel (Frequency Division Multiple Access) ; chaque canal (unidirectionnel) occupe une bande passante de 200 kHz
- TDMA : multiplexage temporel (Time Division Multiple Access) ; chaque canal est divisé en 8 *slots* (*slot = tranche, créneau*)

Trames GSM

- Débit brut: 270.8 kbps (kilobits par seconde), par modulation GMSK (Gaussian Minimum Shift keying)
- Une multitrame comporte 26 trames, soit 32 500 bits transmis en 120 ms.
- 24 trames pour la voix ou les données, 1 trame pour la signalisation, 1 trame pour les SMS et autres trafics spéciaux (numéro appelant, etc.)
- Une *trame* comporte 1250 bits, émis en 120 / 26 ≅ 4.6 ms
- Un *slot* comporte 1250 / 8 = 156.25 bits (sic !), émis en 15 / 26 ≅ 0.577 ms , soit 577 • s

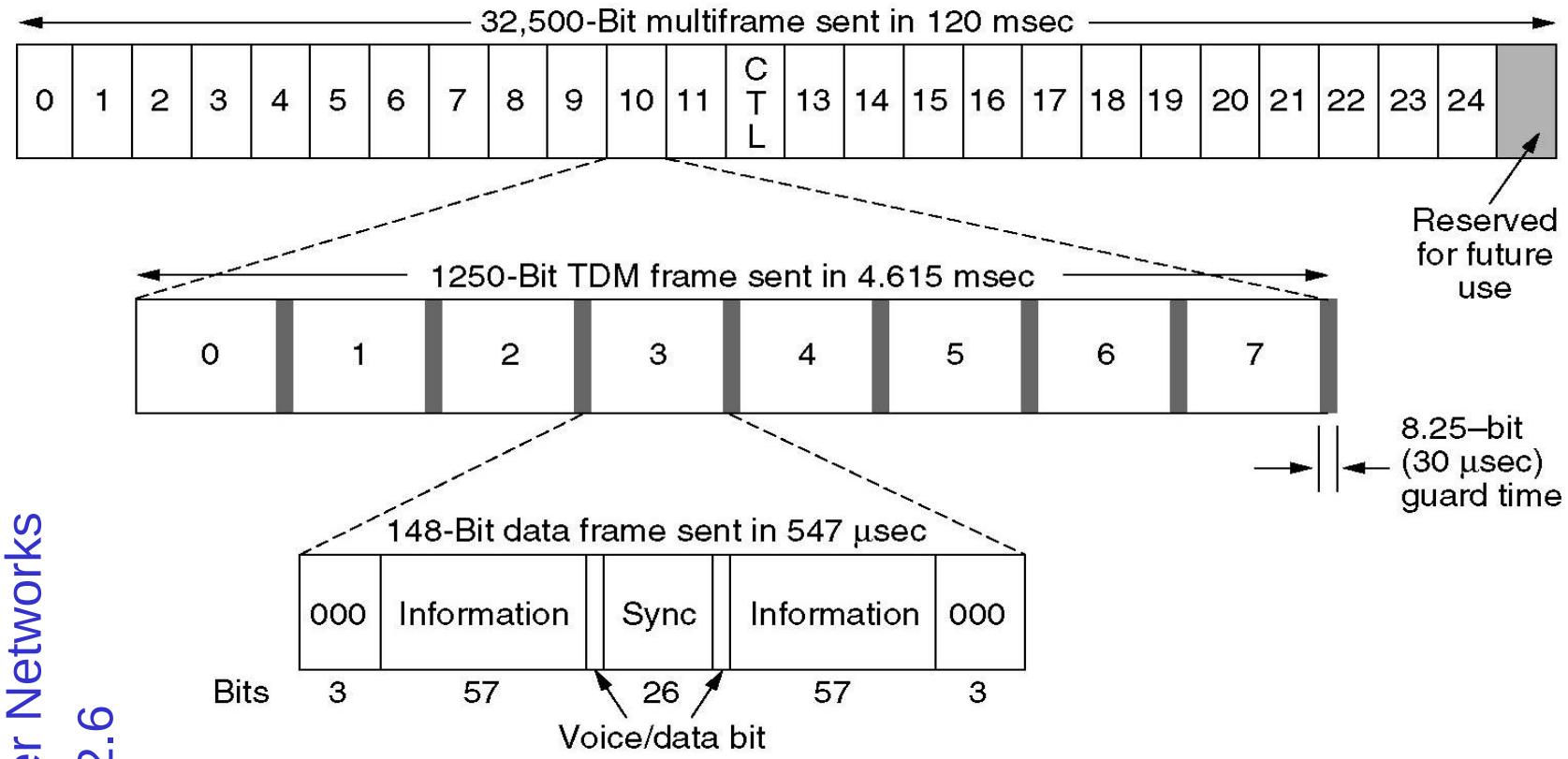
FDMA + TDMA

Tanenbaum, Computer Networks, section 2.6



GSM uses 124 frequency channels, each of which uses an eight-slot TDM system

GSM Framing Structure



A portion of the GSM framing structure.

R. Levine

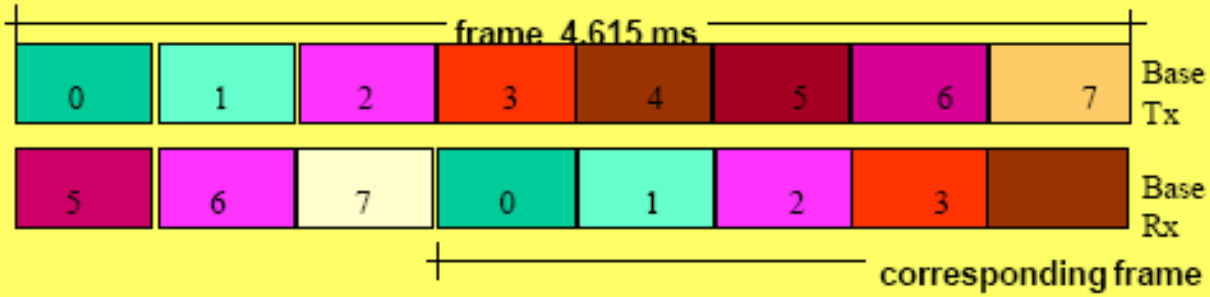
Digital Switching

Lectures April 17 & 24, 2001
Cellular & PCS

Two suggested reference books by L.Harte and R. Levine :
***Cellular and PCS: The Big Picture* (1997)**
***GSM SuperPhones* (1999)**
both published by McGraw-Hill

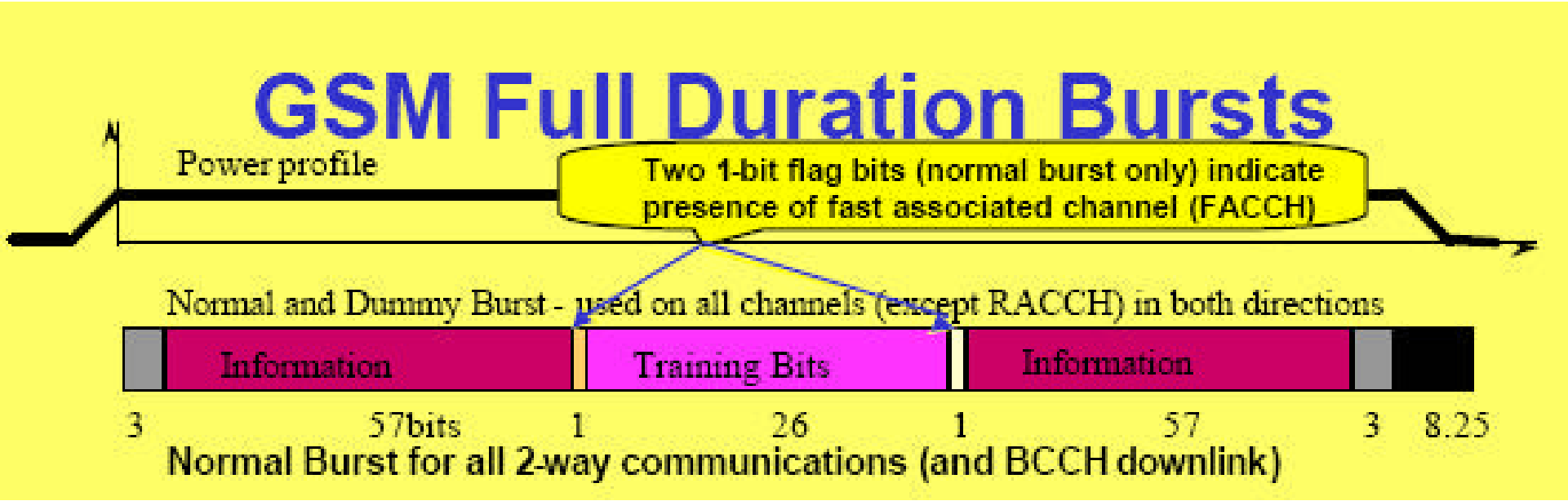
Trame GSM

GSM TDMA Frame and Slot

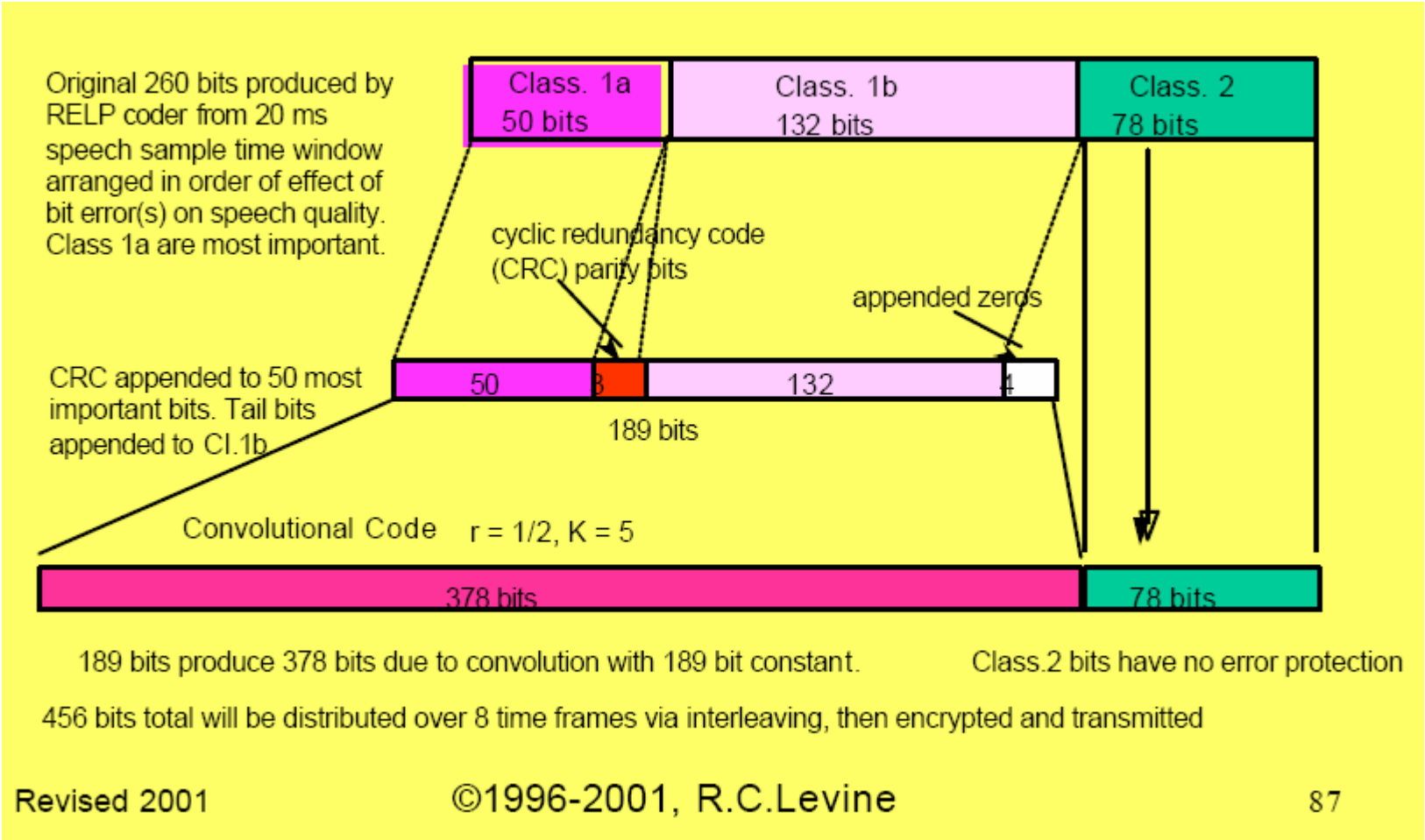


- Base Tx frame start is advanced 3 slots from logically corresponding Base Rx frame start with corresponding slot number
  - Mobile set using a designated slot first receives, then waits 2 slots, then transmits, then waits for 4 "idle" time slots, then repeats
    - Mobile can do other things in 6 "idle" slots (like MAHO)
  - Mobile set does *not* transmit and receive simultaneously when using only 1 time slot for digitally coded voice communication
  - Mobile can make small Tx timing adjustments, in response to base commands, to adjust for 3.3µs/km one-way (6.6 µs/km 2-way) radio signal delay

Slot GSM


GSM Full Duration Bursts
Power profile
Two 1-bit flag bits (normal burst only) indicate presence of fast associated channel (FACCH)
Normal and Dummy Burst - used on all channels (except RACCH) in both directions
Information
Training Bits
Information
3
57bits
1
26
1
57
3
8.25
Normal Burst for all 2-way communications (and BCCH downlink)

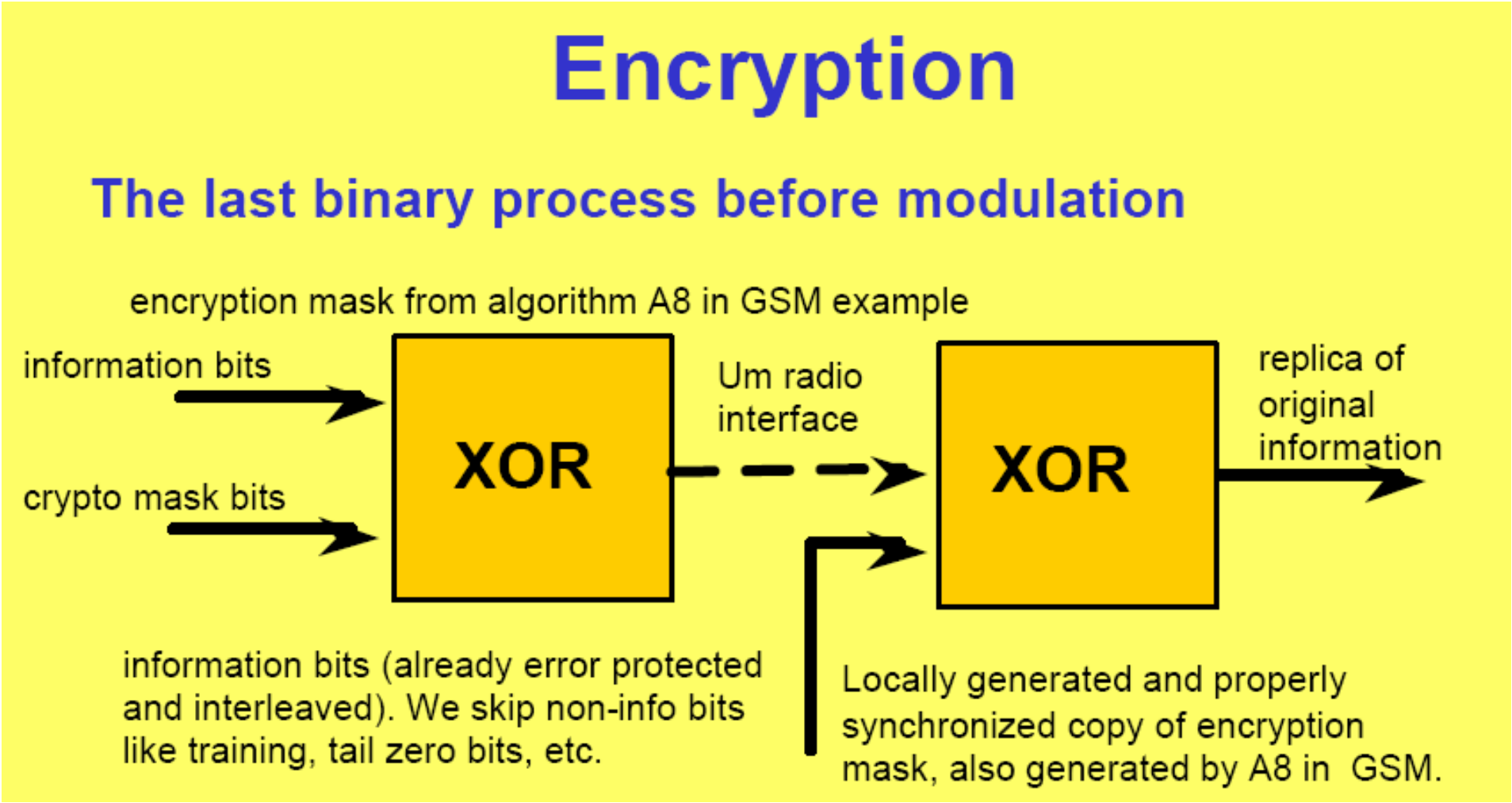
Codes détecteurs/correcteurs d’erreurs



Codes (2)

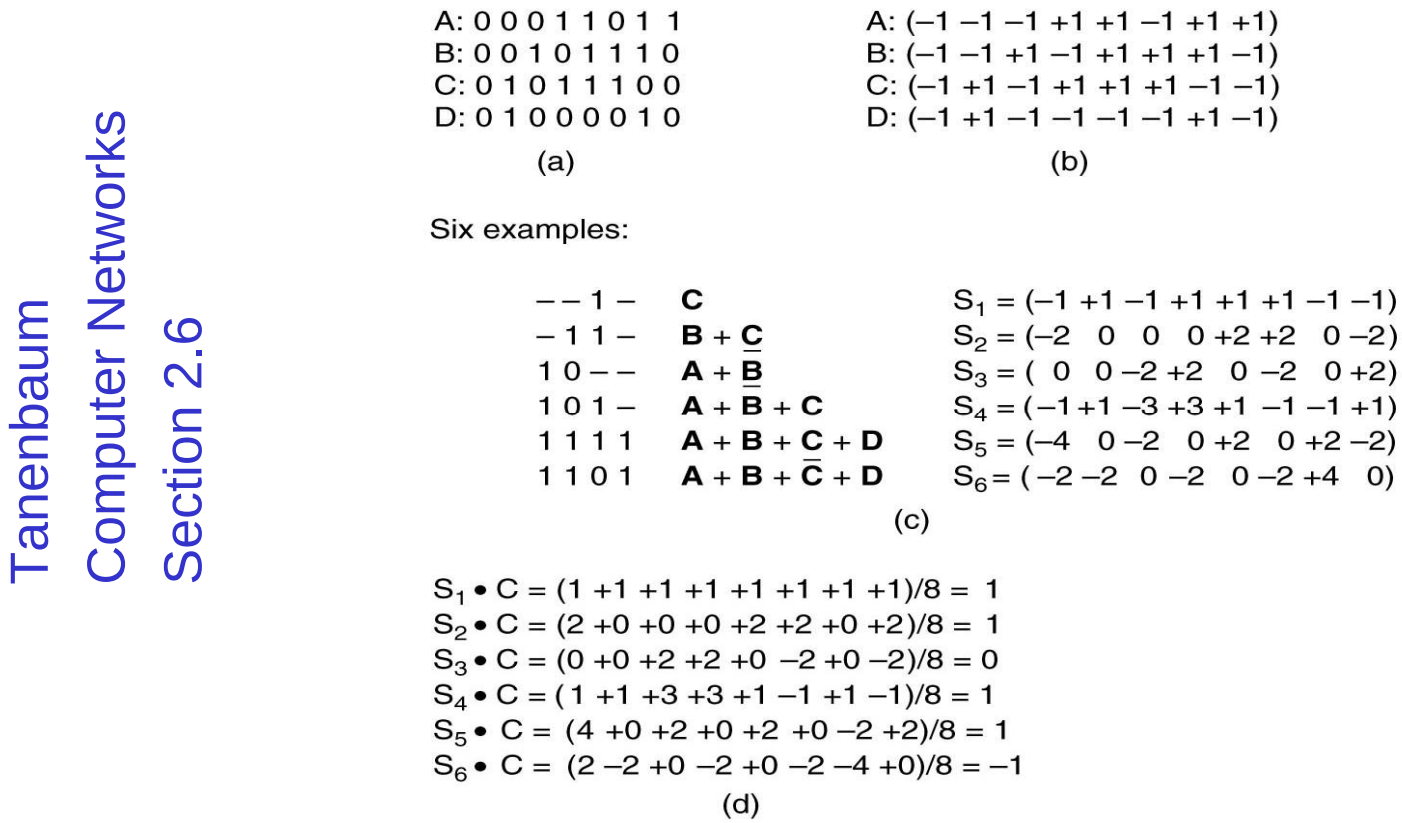
- The 3-bit CRC permits correction of single bit errors in the 50 most protected bits all by itself.
- The convolution code can correct several bit errors, and detect any bursts of errors which are within a consecutive group of 5 bits.
- Most of the bits in Classes 1a and 1b are most significant bits of filter coefficients and other numerical bit quantities which have an obvious significant effect on the sound output if they are wrong.
- Most Cl.2 bits are least significant bits of numeric quantities and some bits describing the excitation waveform.

Chiffrement



CDMA – Code Division Multiple Access

Tanenbaum Computer Networks Section 2.6



(a) Binary chip sequences for four stations
(b) Bipolar chip sequences
(c) Six examples of transmissions
(d) Recovery of station C's signal