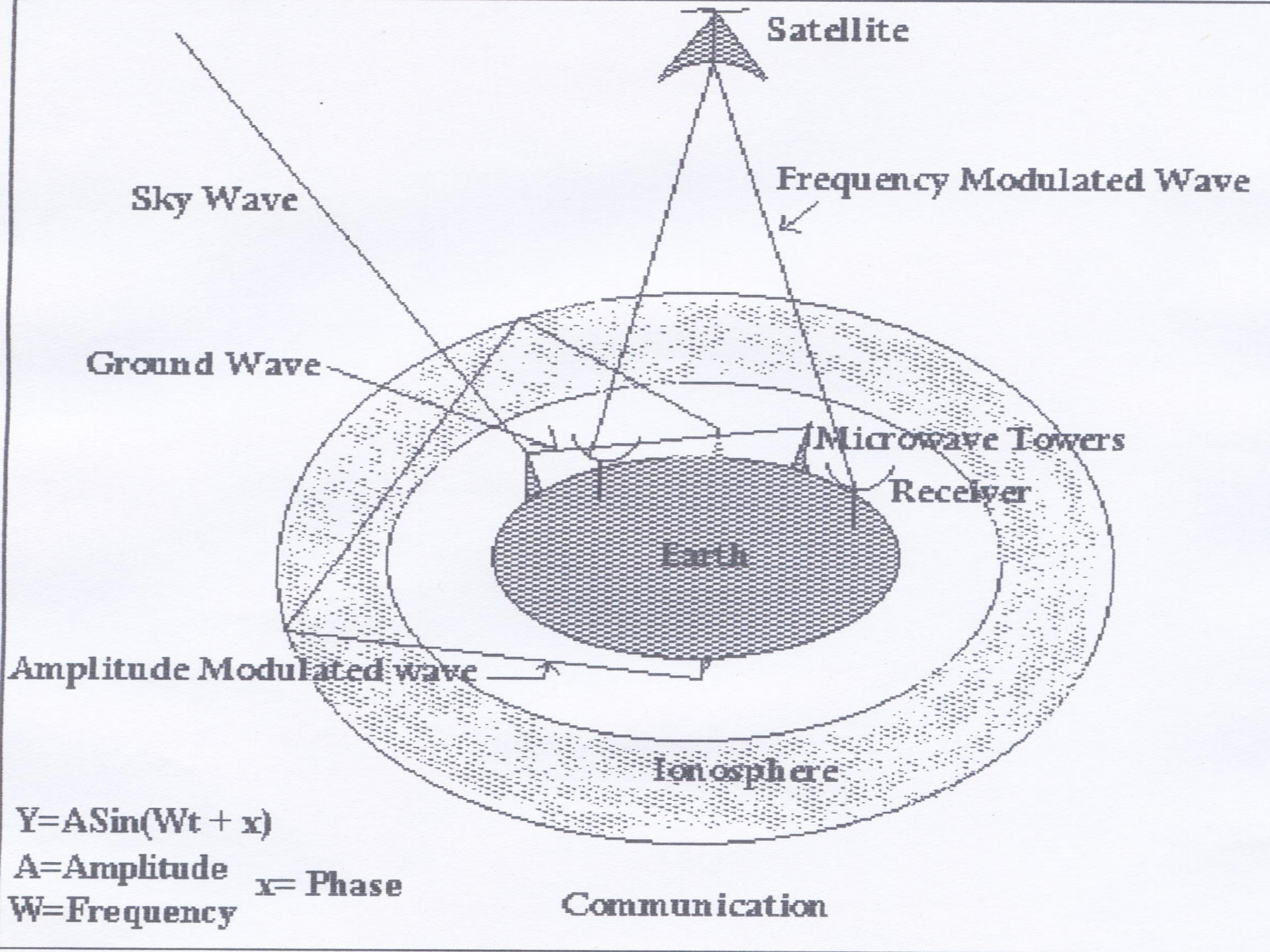
Security
in
Wireless Communication

Prof.(Dr.) J. K. Mandal

UNIVERSITY OF KALYANI, KALYANI, NADIA, INDIA

Jkm.cse@gmail.com



Y=ASin(Wt + x)

A=Amplitude

W=Frequency

x= Phase

Communication

Types of Transmission

- **Guided Transmission**
- **Unguided Transmission**

Figure 7.1 *Transmission medium and physical layer*

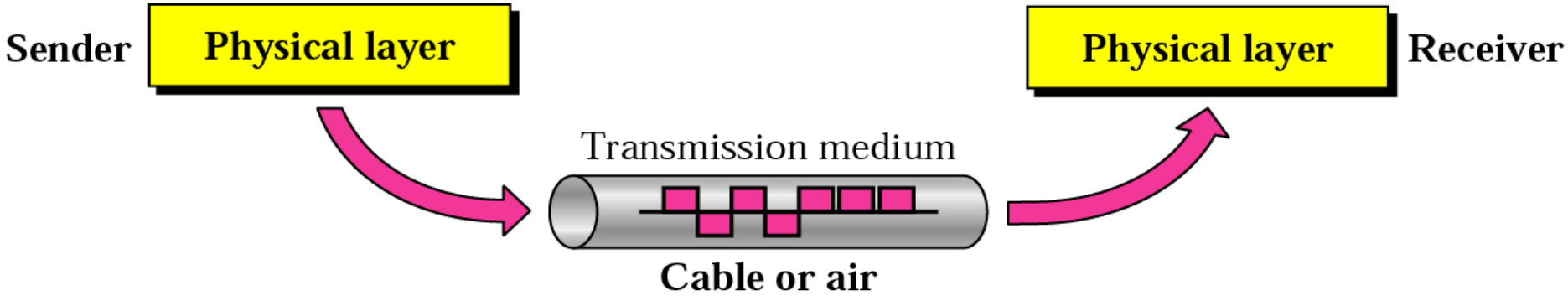
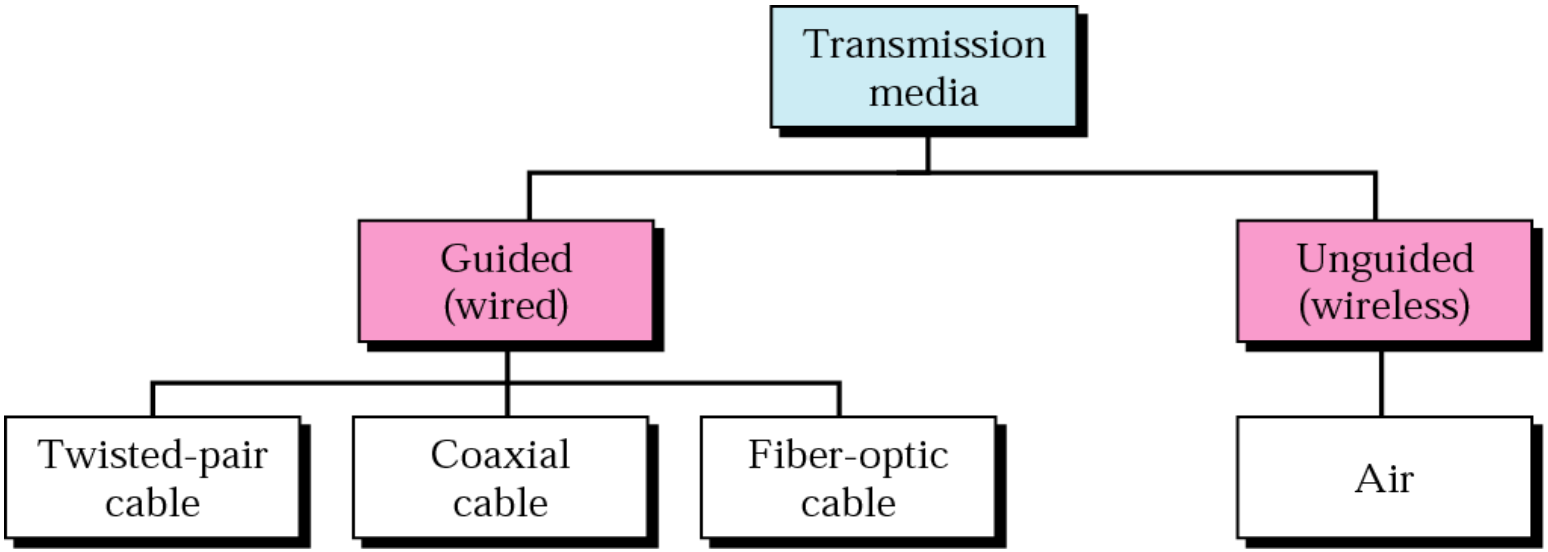


Figure 7.2 Classes of transmission media



Guided Transmission

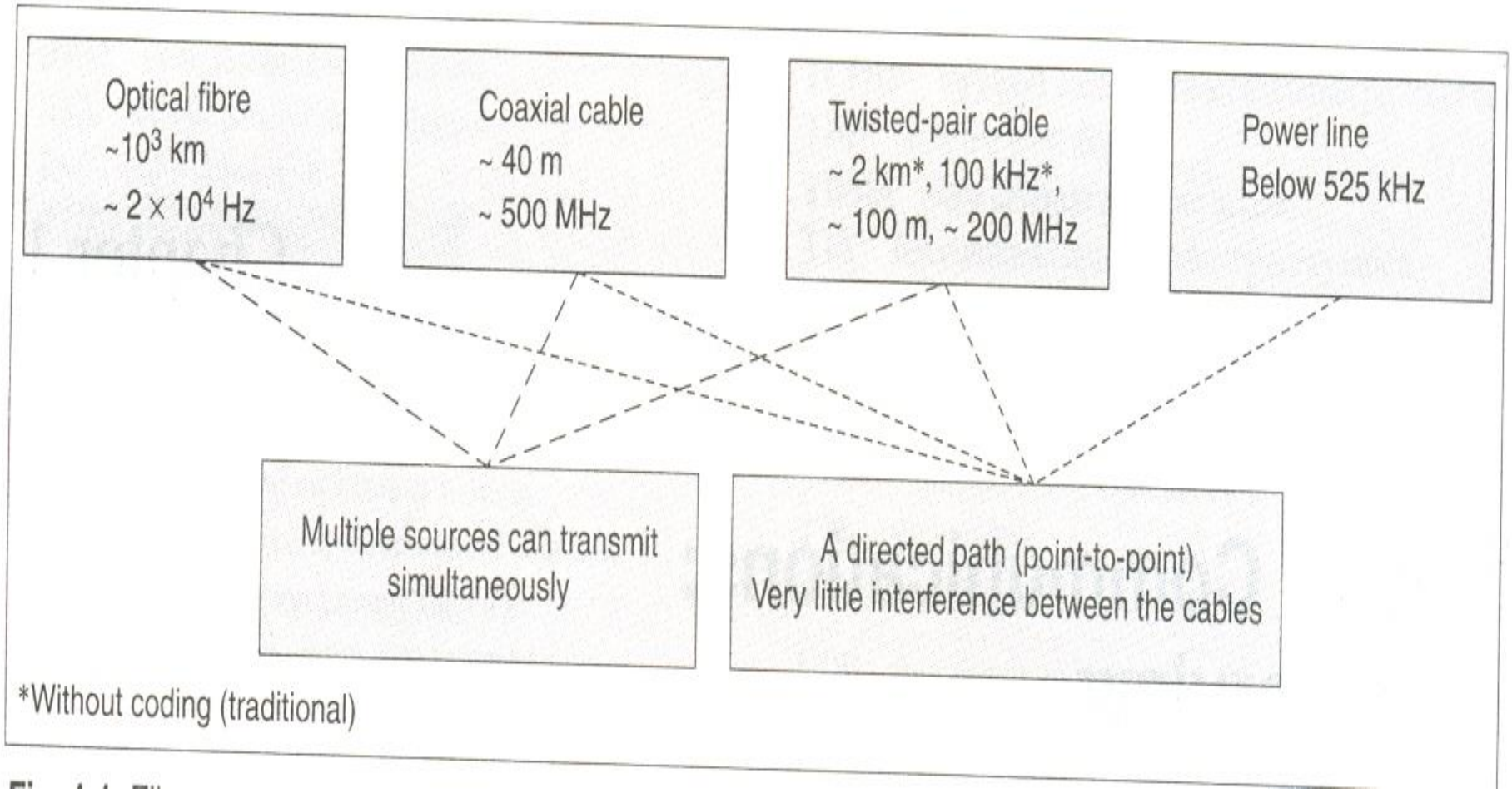
Metal wires and optical fibres are used in guided or wired transmission of data. Figure 1.1 shows the fibre- and wire-based communication frequencies and the main properties of this mode of transmission. Guided transmission of electrical signals takes place using four types of cables-

(i) optical fibre for pulses of wavelength 1.35-1.5 μm,

(ii) coaxial cable for electrical signals of frequencies up to 500 MHz and up to a range of about 40 m,

(iii) twisted wire pairs for conventional (without coding) electrical signals of up to 100 kHz and up to a range of 2 km, or for coded signals of frequencies up to 200 MHz and a range of about 100 m, and

(iv) power lines, a relatively recent advent in communication technology, are used for long-range transmission of frequencies between 10 kHz and 525 kHz.



Fibre- and wire-based transmissions and their ranges (without using repeater), frequencies, and properties.

Advantages & disadvantages

- The advantages of cable-based transmission are-
  (a)transmission is along a directed path from one point to another,
  (b)there is practically no interference in transmission from any external source or path, and
  (c)using multiplexing and coding, a large number of signal sources can be simultaneously transmitted along an optical fibre, a coaxial cable, or a twisted-pair cable.

- Significant disadvantages of transmission through cables are:
  (a)Signal transmitter and receiver are fixed (immobile). Hence there is no mobility of transmission and reception points.
  (b)The number of transmitter and receiver systems limits the total number of user

Unguided Transmission

Wireless or unguided transmission is carried out through radiated electromagnetic energy

7.1 Guided Media

Twisted-Pair Cable

Coaxial Cable

Fiber-Optic Cable

Figure 7.3 *Twisted-pair cable*

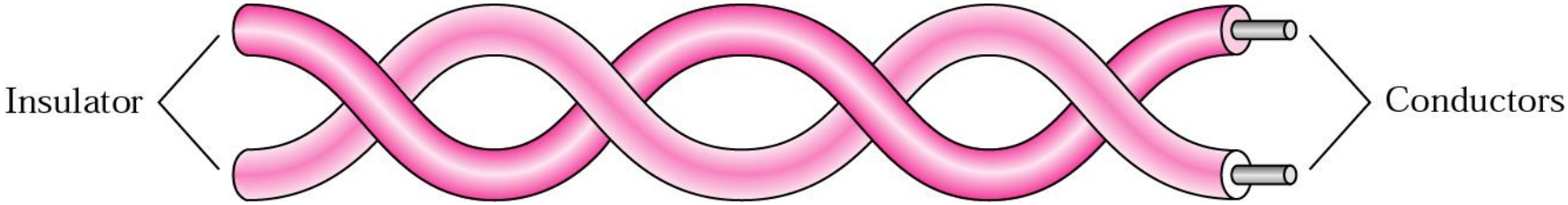
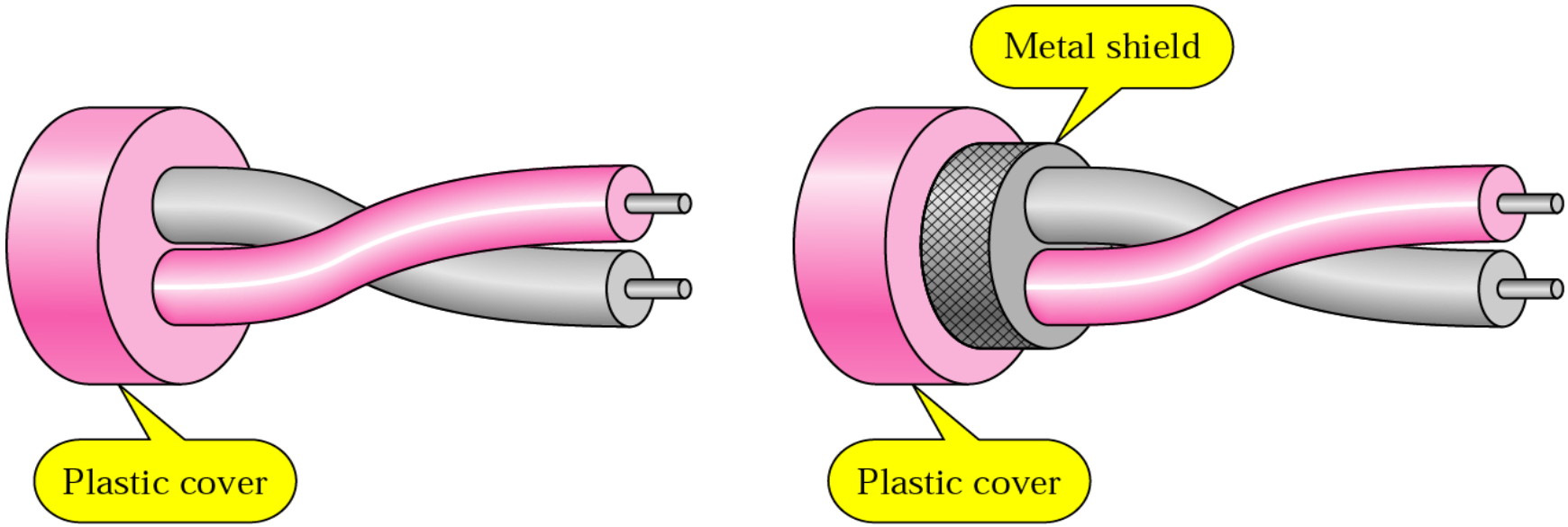


Figure 7.4 *UTP and STP*



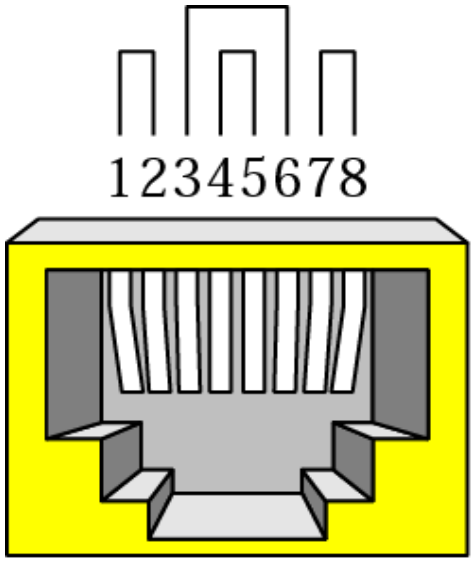
a. UTP

b. STP

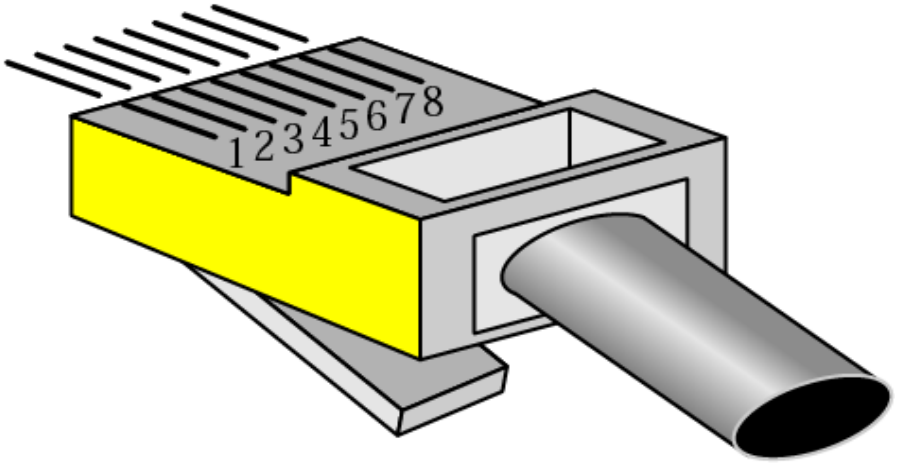
Table 7.1 Categories of unshielded twisted-pair cables

Category	Bandwidth	Data Rate	Digital/Analog	Use
1	very low	< 100 kbps	Analog	Telephone
2	< 2 MHz	2 Mbps	Analog/digital	T-1 lines
3	16 MHz	10 Mbps	Digital	LANs
4	20 MHz	20 Mbps	Digital	LANs
5	100 MHz	100 Mbps	Digital	LANs
6 (draft)	200 MHz	200 Mbps	Digital	LANs
7 (draft)	600 MHz	600 Mbps	Digital	LANs

Figure 7.5 *UTP connector*



RJ-45 Female



RJ-45 Male

Figure 7.6 *UTP performance*

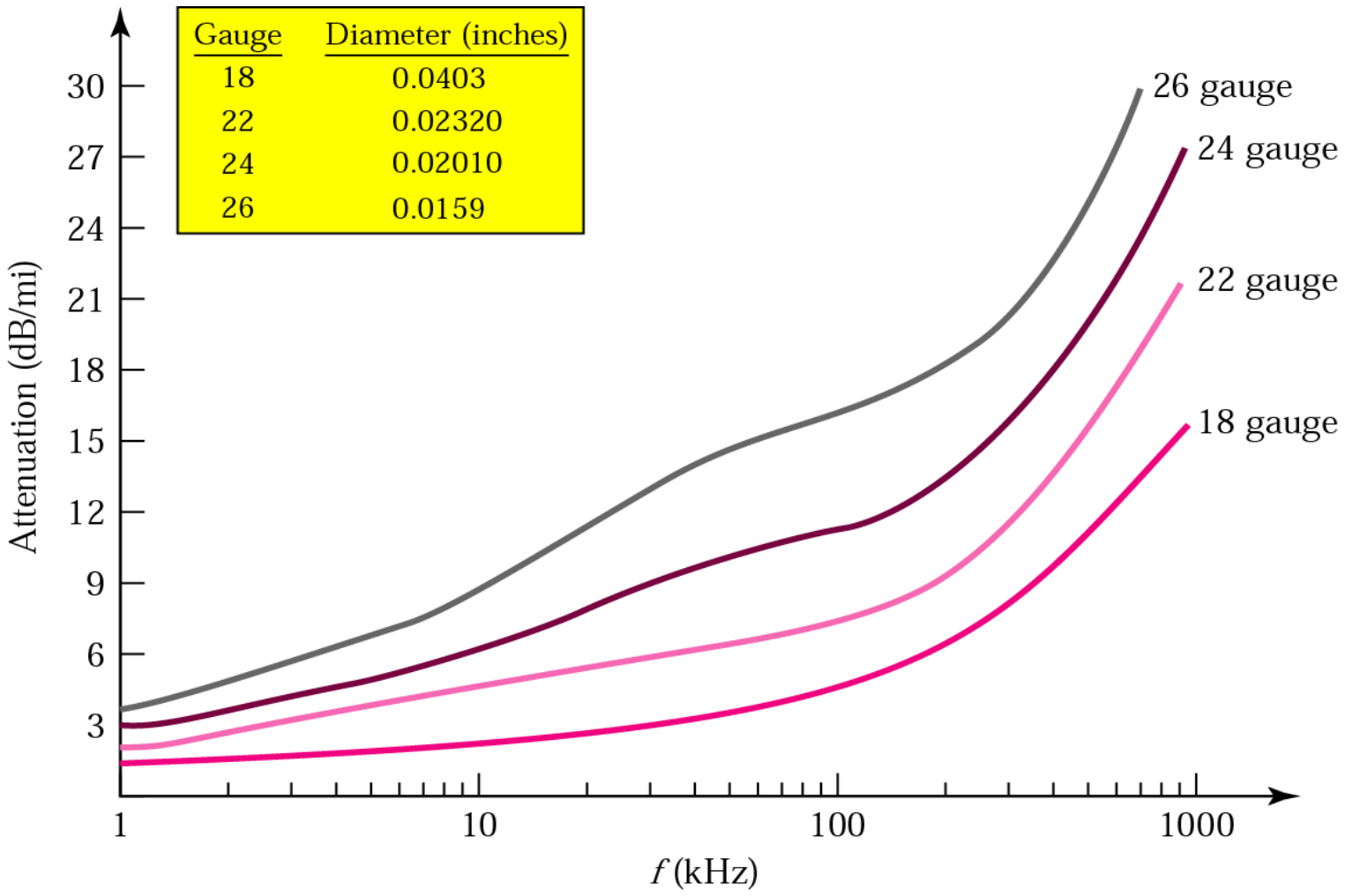


Figure 7.7 *Coaxial cable*

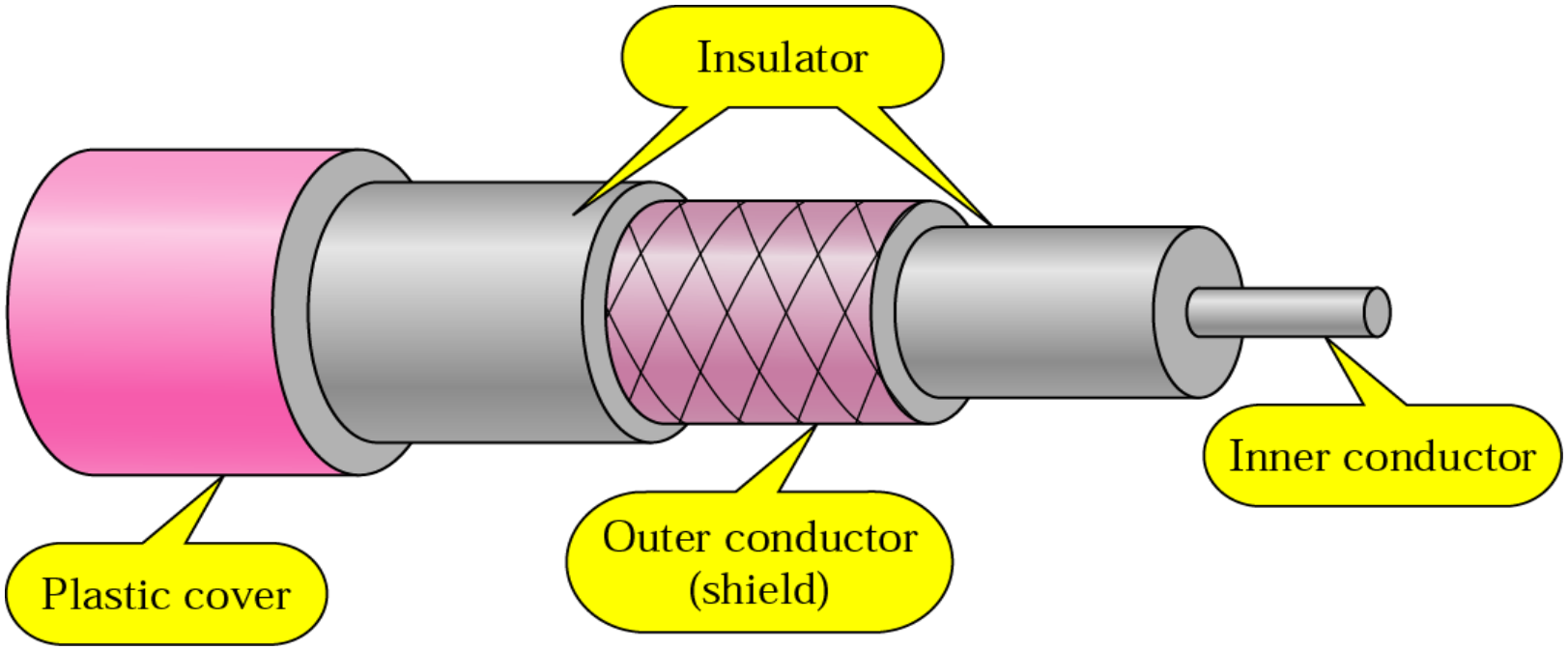


Table 7.2 Categories of coaxial cables

Category	Impedance	Use
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Figure 7.8 *BNC connectors*

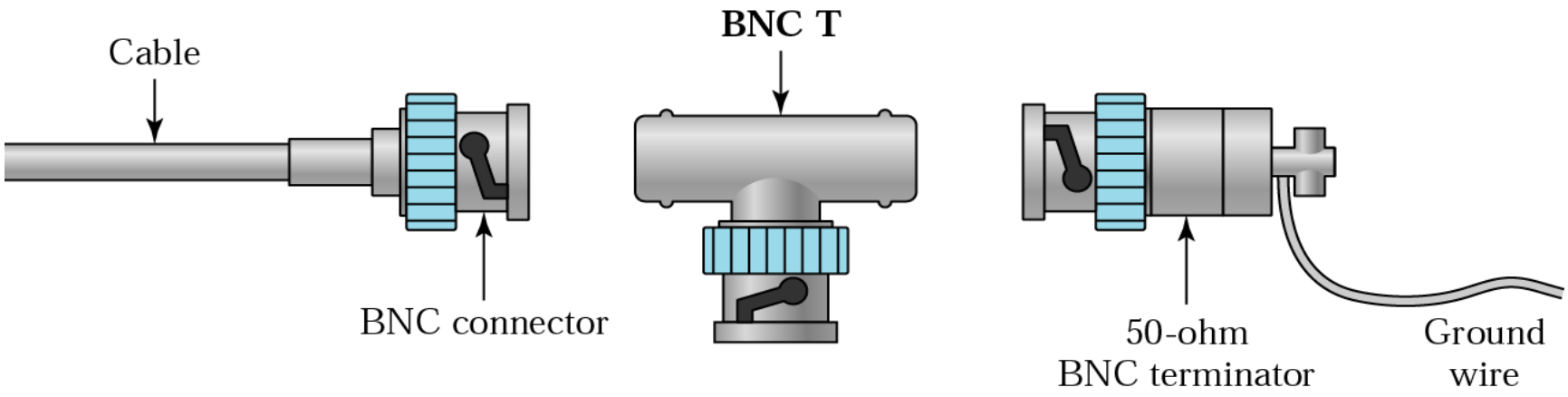


Figure 7.9 *Coaxial cable performance*

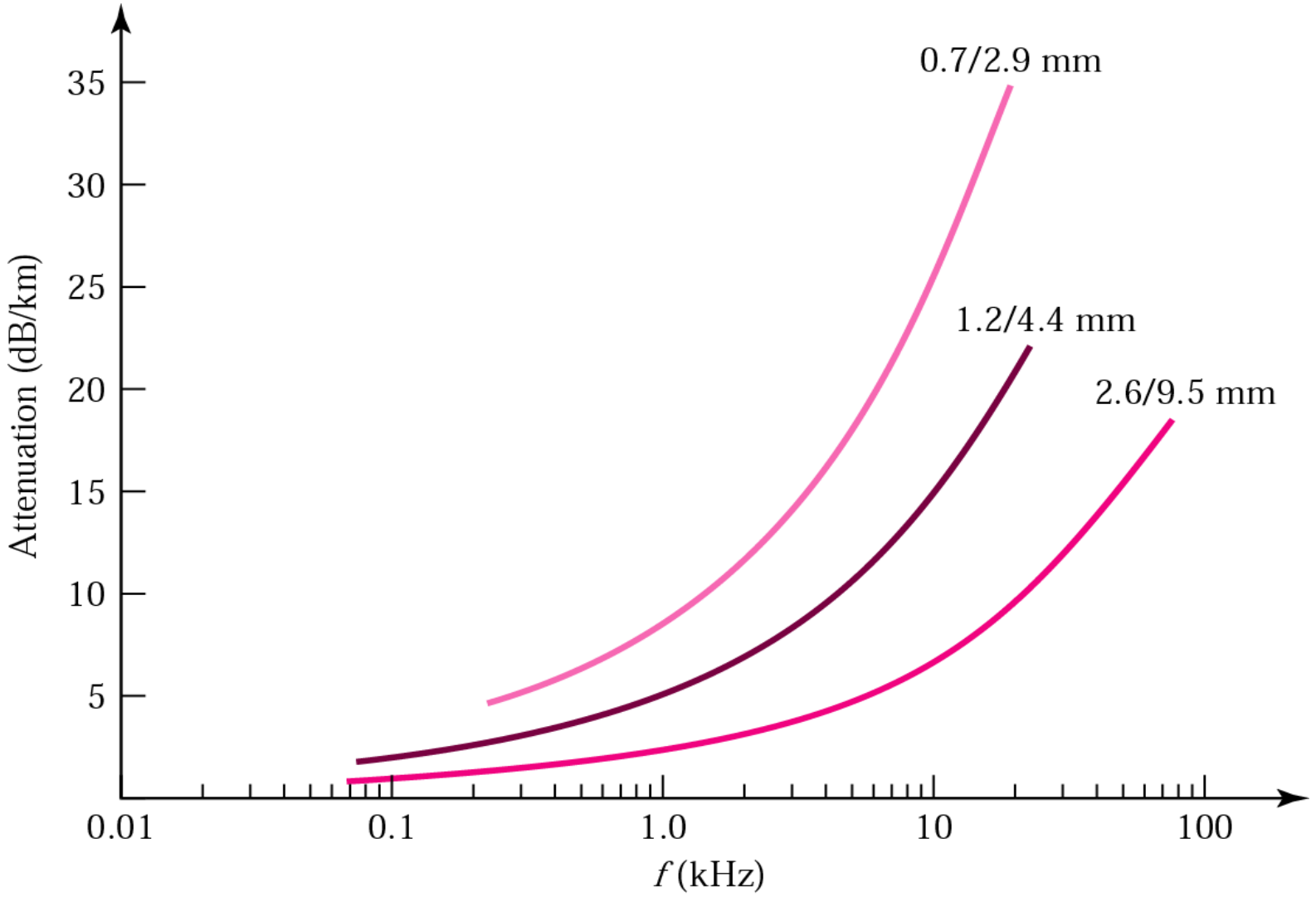
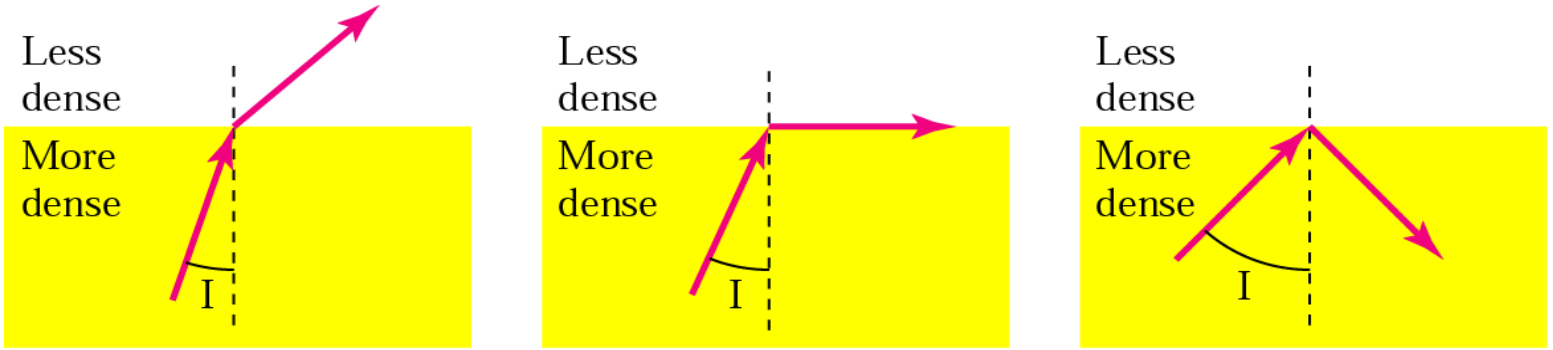


Figure 7.10 *Bending of light ray*



I < critical angle, refraction

I = critical angle, refraction

I > critical angle, reflection

Figure 7.11 *Optical fiber*

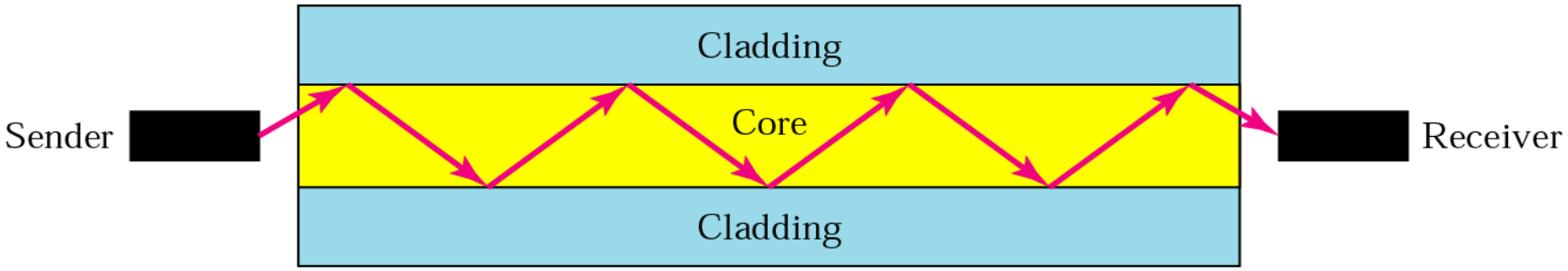


Figure 7.12 *Propagation modes*

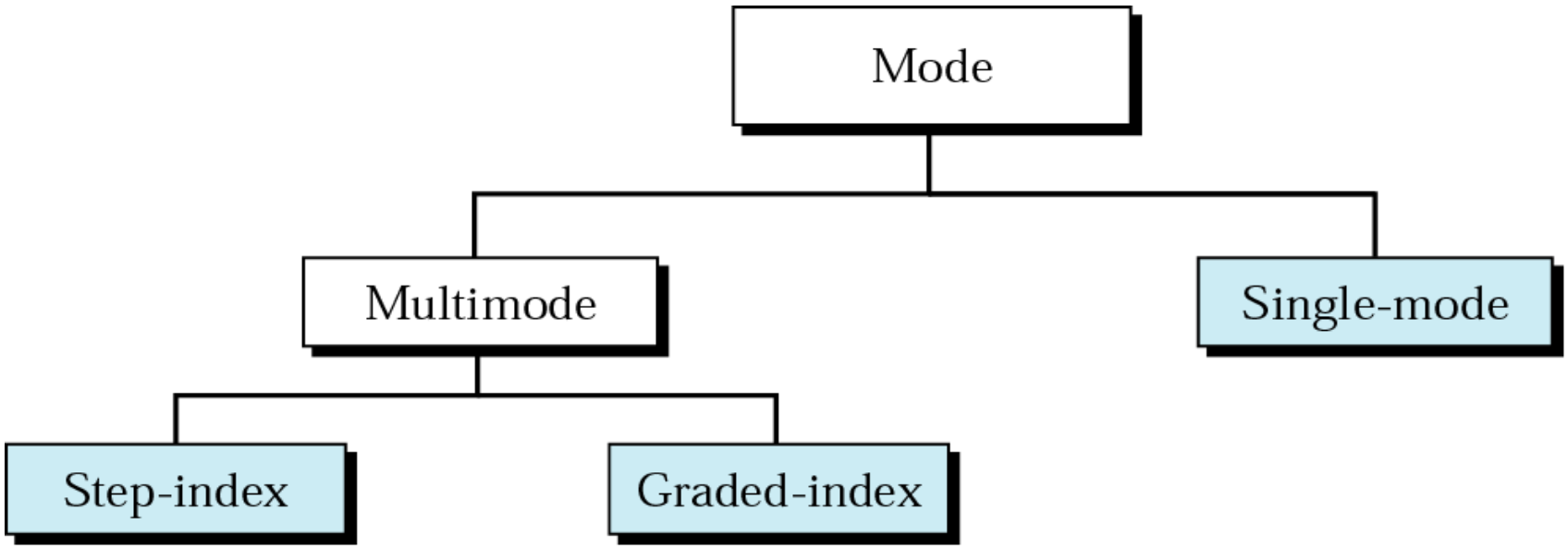


Figure 7.13 *Modes*

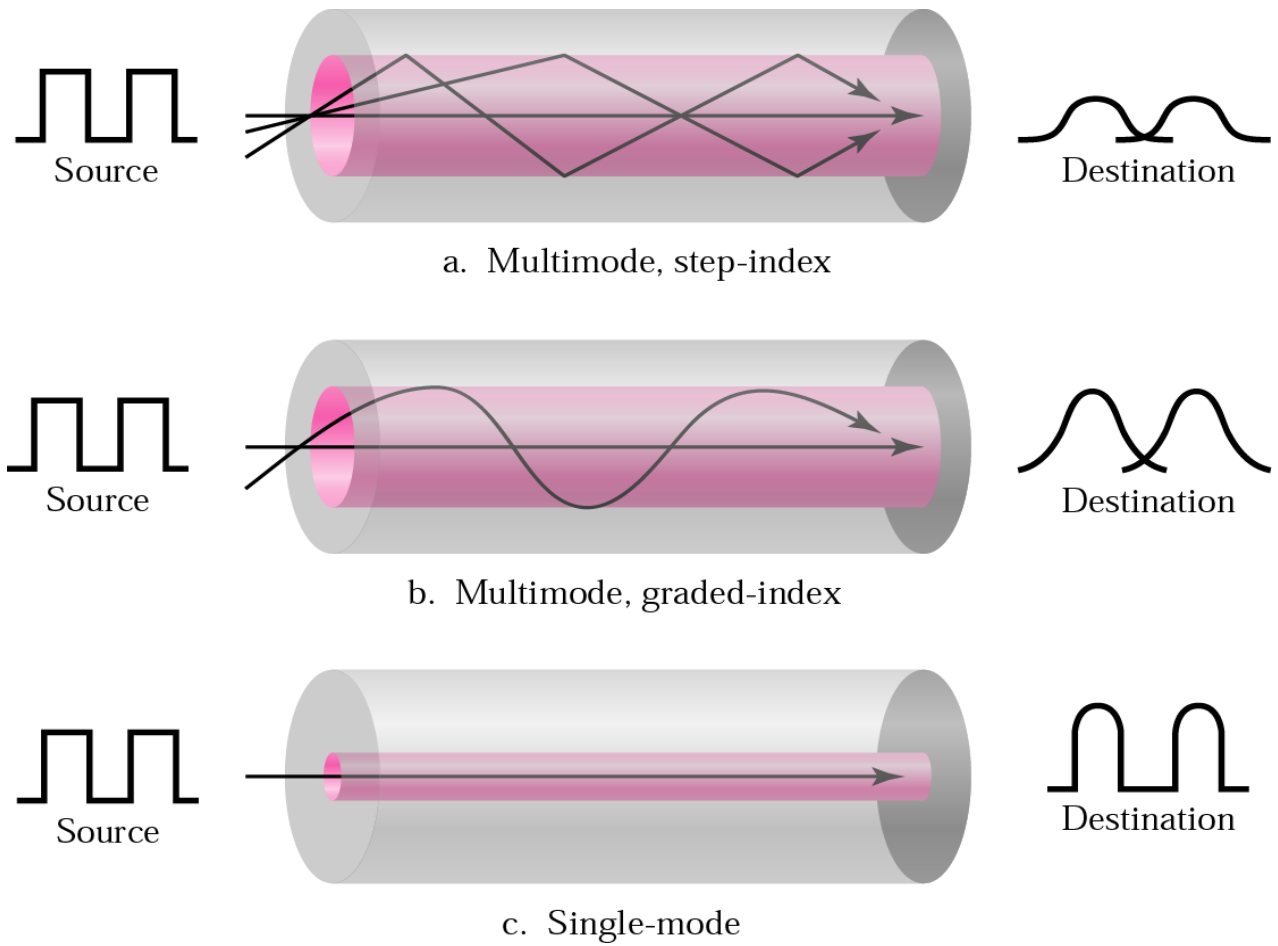


Table 7.3 Fiber types

Type	Core	Cladding	Mode
50/125	50	125	Multimode, graded-index
62.5/125	62.5	125	Multimode, graded-index
100/125	100	125	Multimode, graded-index
7/125	7	125	Single-mode

Figure 7.14 *Fiber construction*

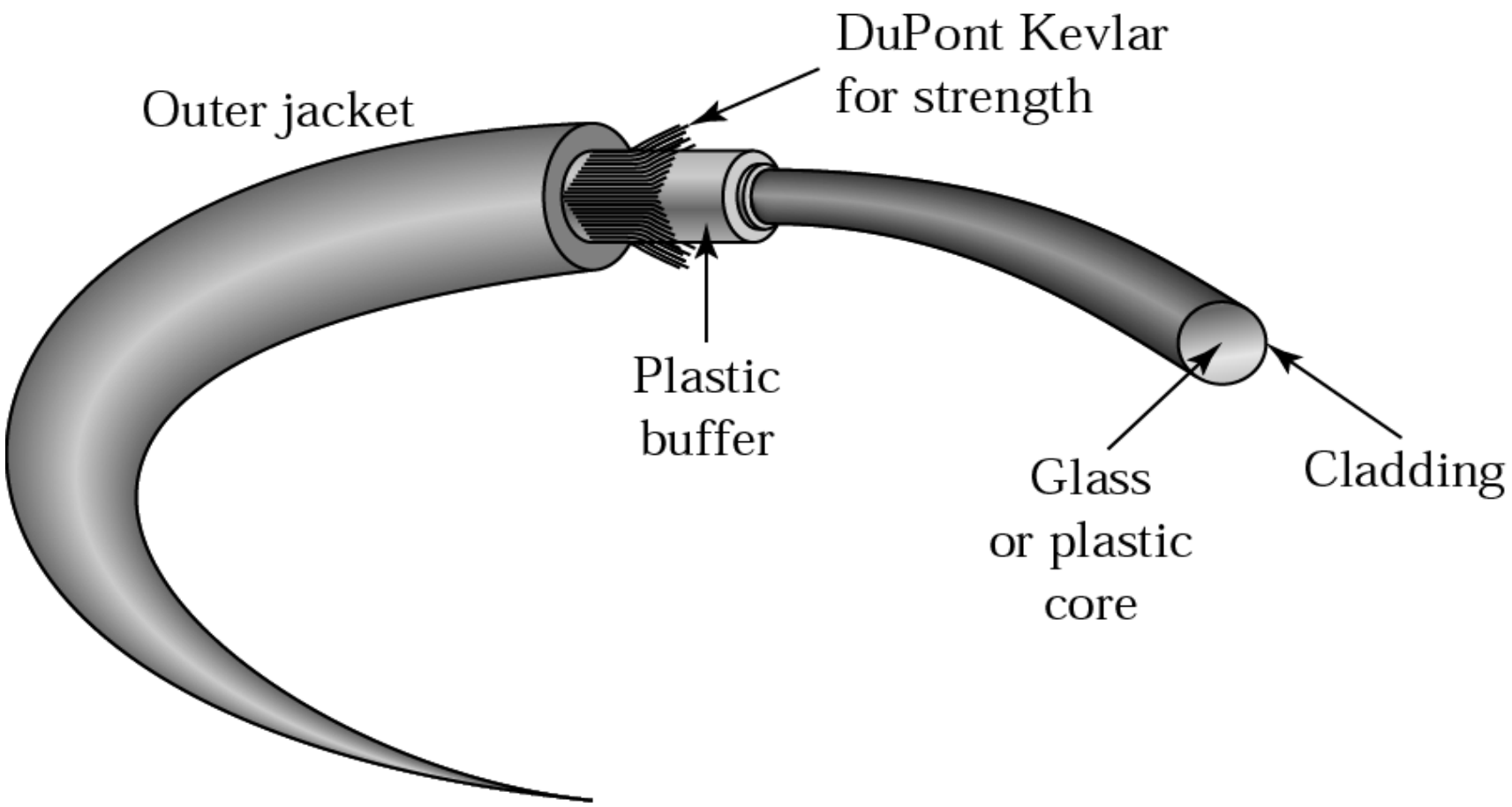


Figure 7.15 *Fiber-optic cable connectors*

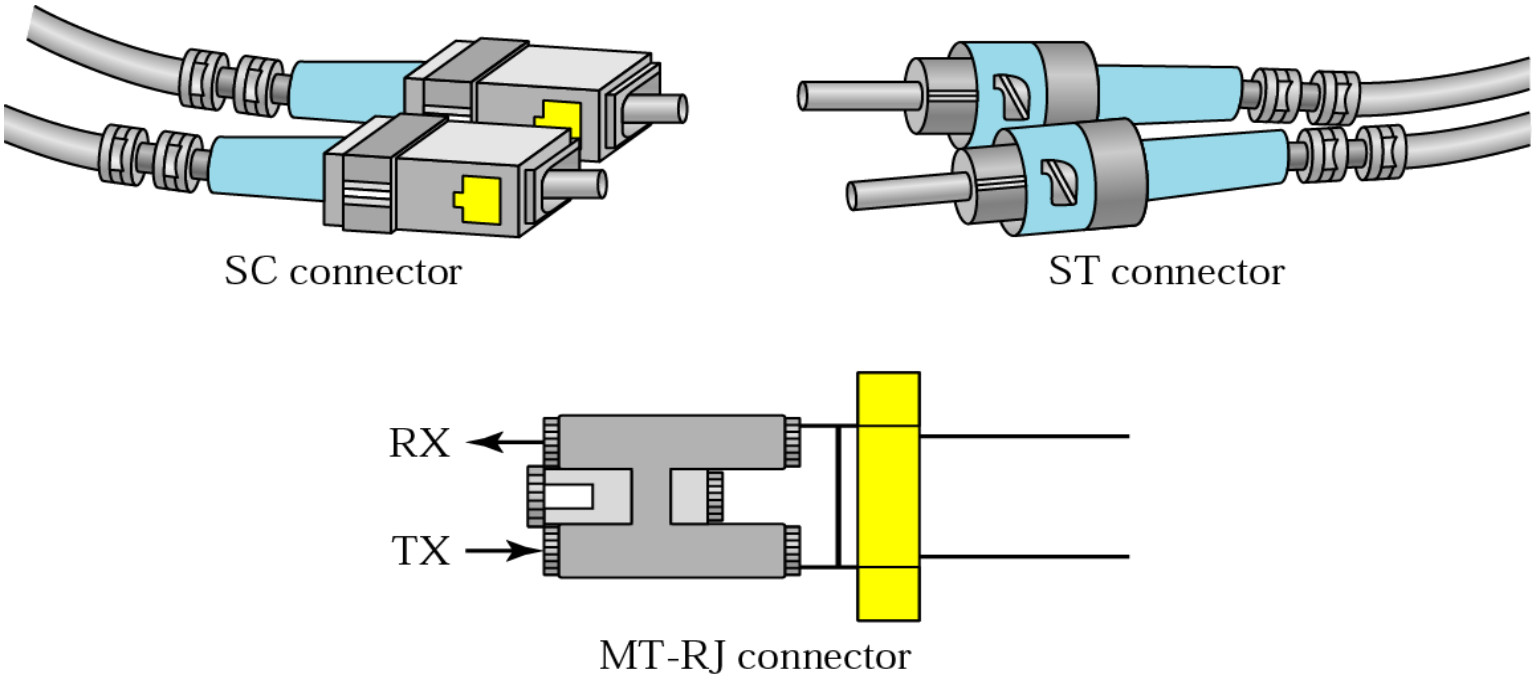
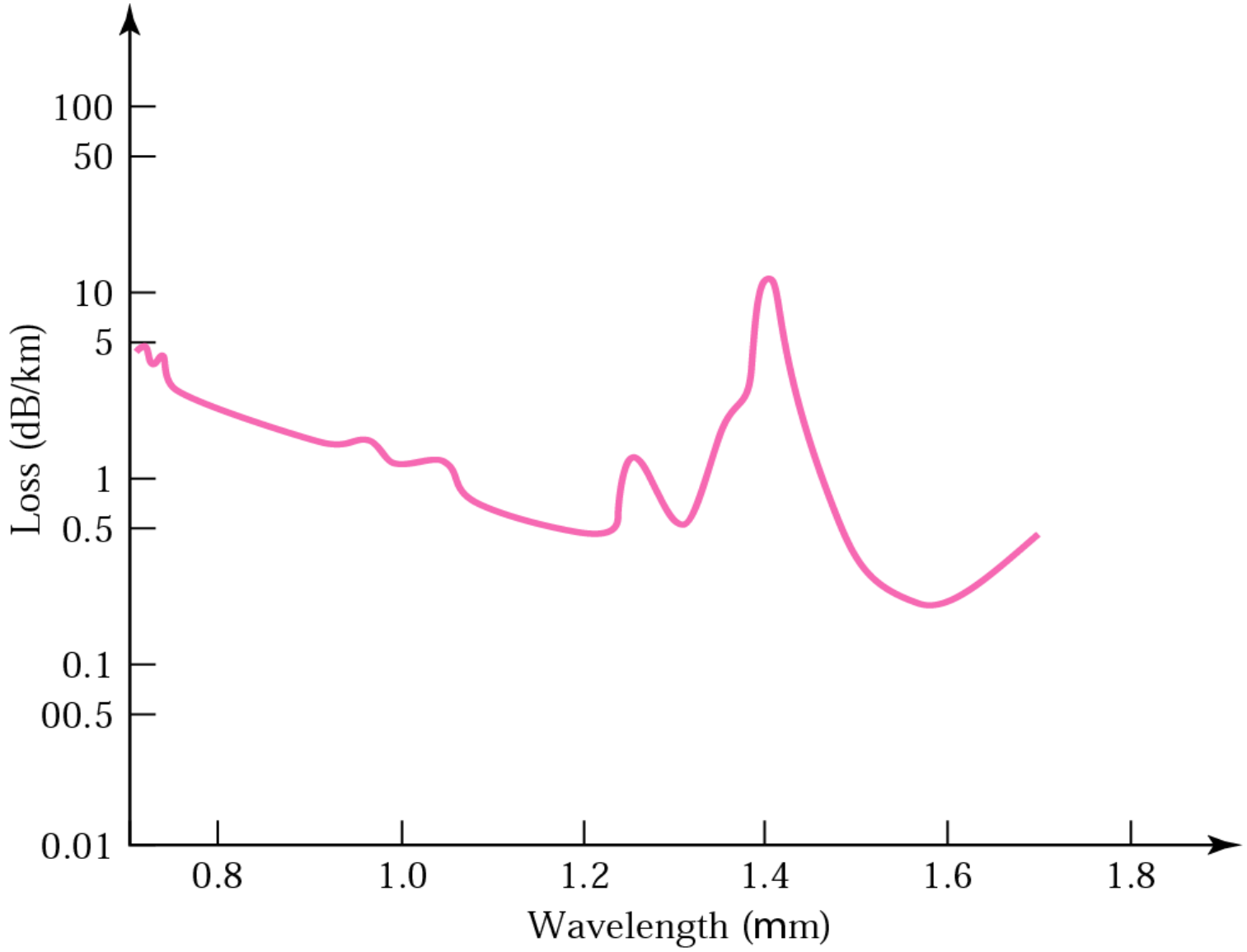


Figure 7.16 *Optical fiber performance*



7.2 Unguided Media: Wireless

Radio Waves

Microwaves

Infrared

Figure 7.17 *Electromagnetic spectrum for wireless communication*

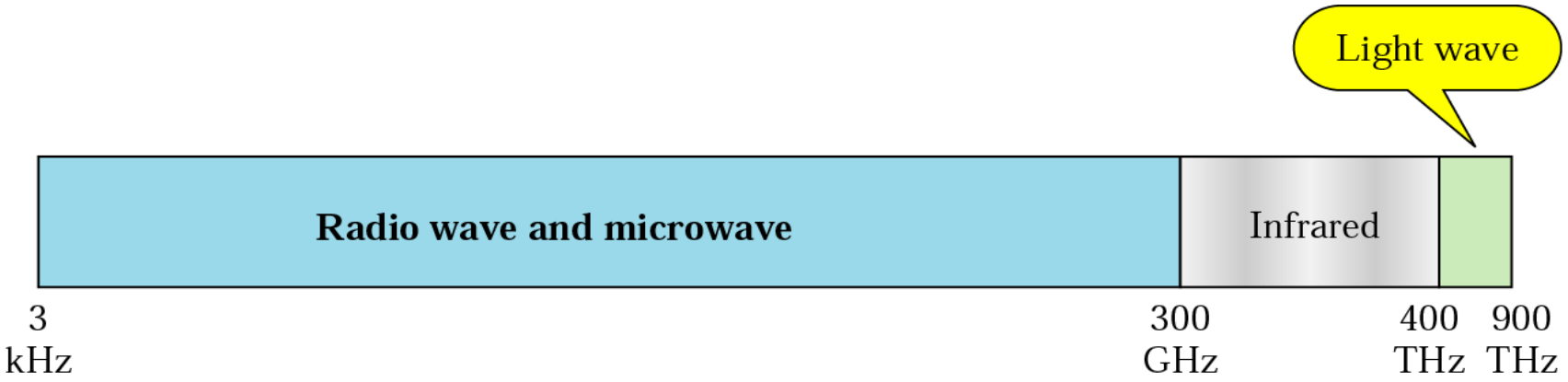


Figure 7.18 *Propagation methods*

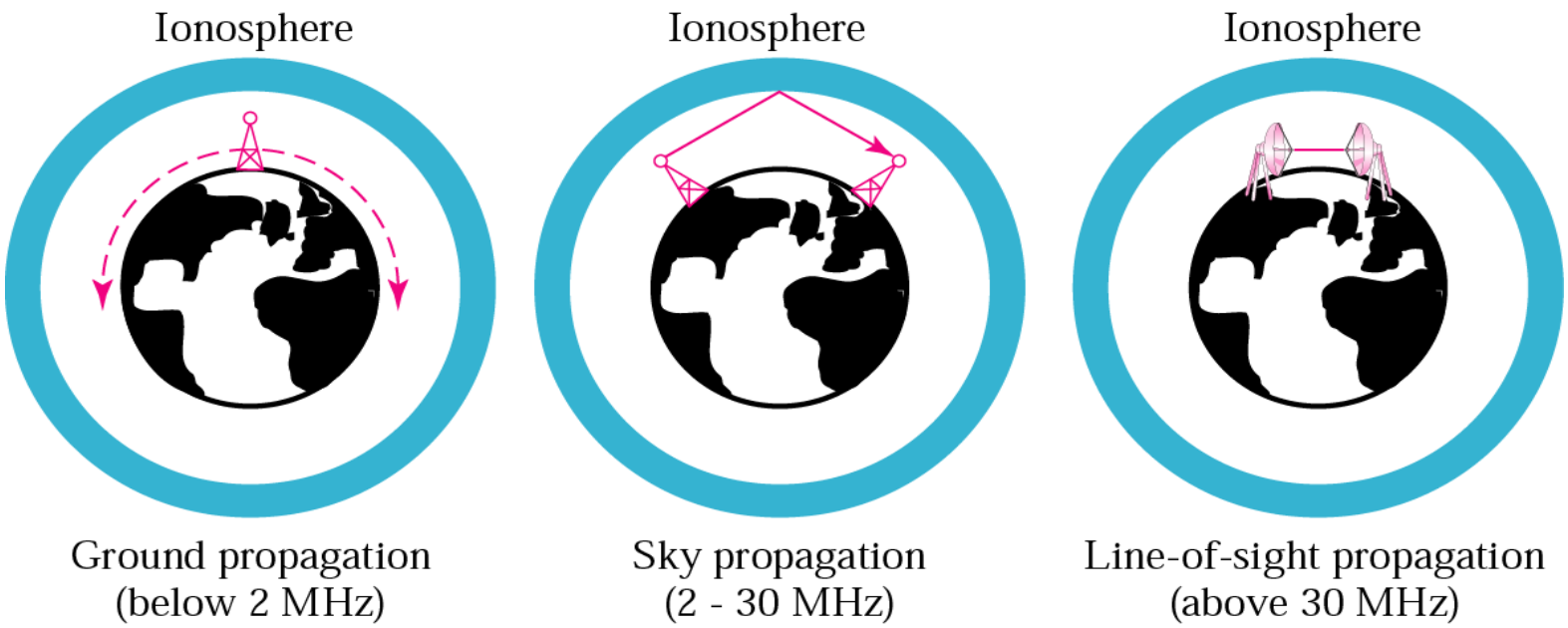


Table 7.4 Bands

Band	Range	Propagation	Application
VLF	3–30 KHz	Ground	Long-range radio navigation
LF	30–300 KHz	Ground	Radio beacons and navigational locators
MF	300 KHz–3 MHz	Sky	AM radio
HF	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF	3–30 GHz	Line-of-sight	Satellite communication
EHF	30–300 GHz	Line-of-sight	Long-range radio navigation

Figure 7.19 *Wireless transmission waves*

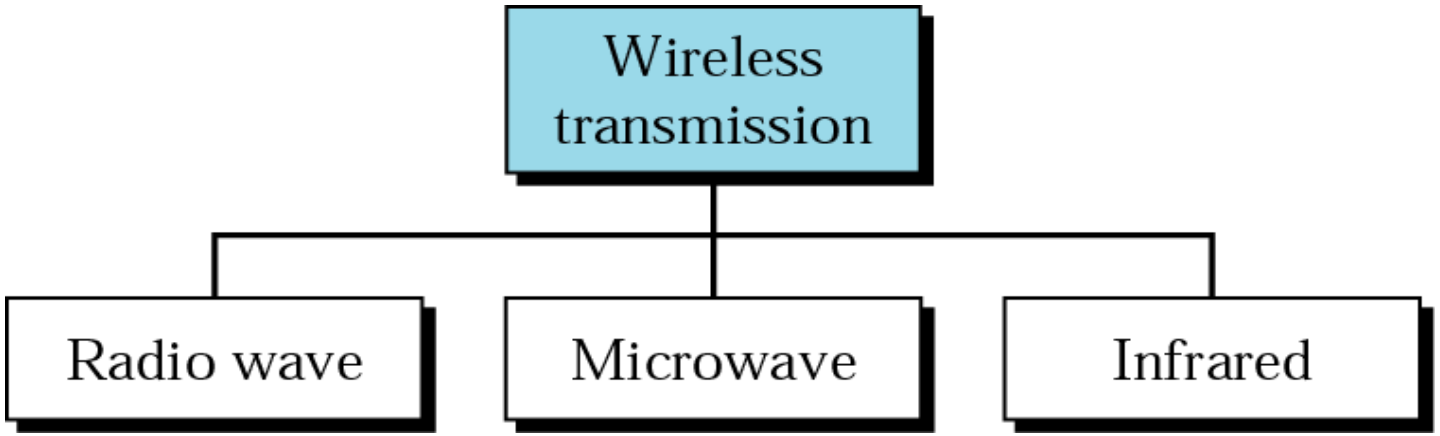
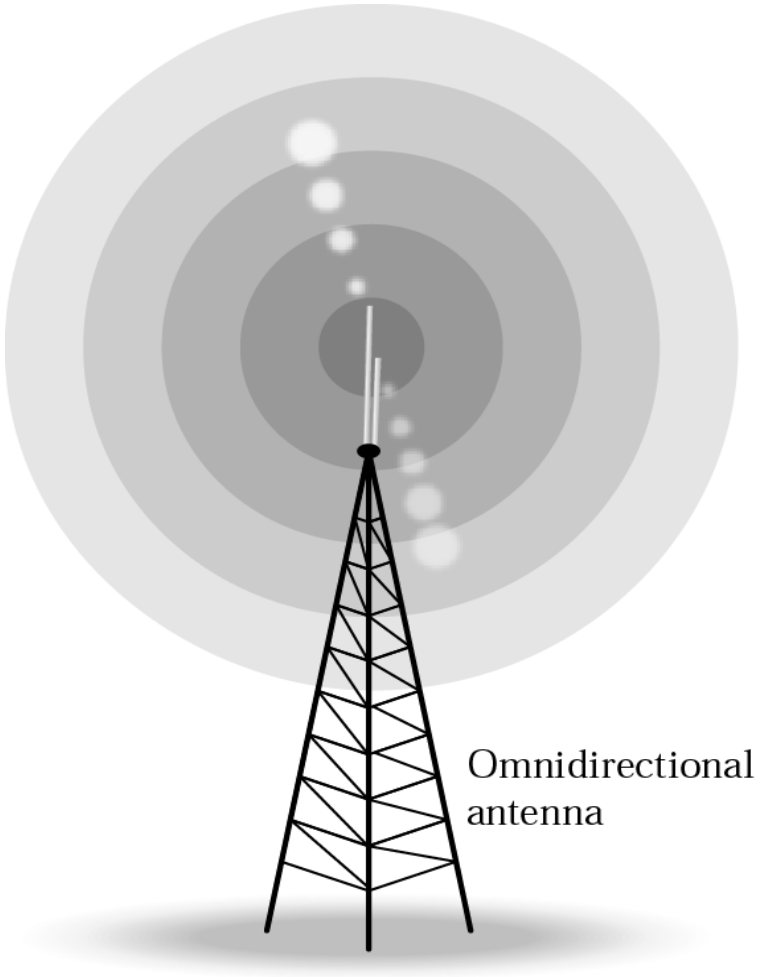
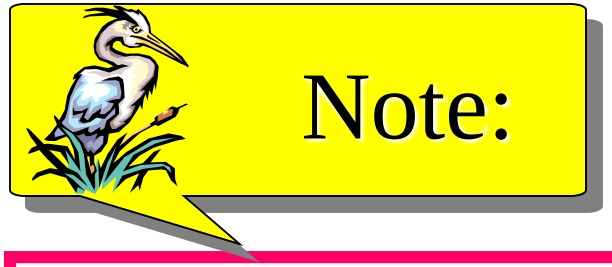


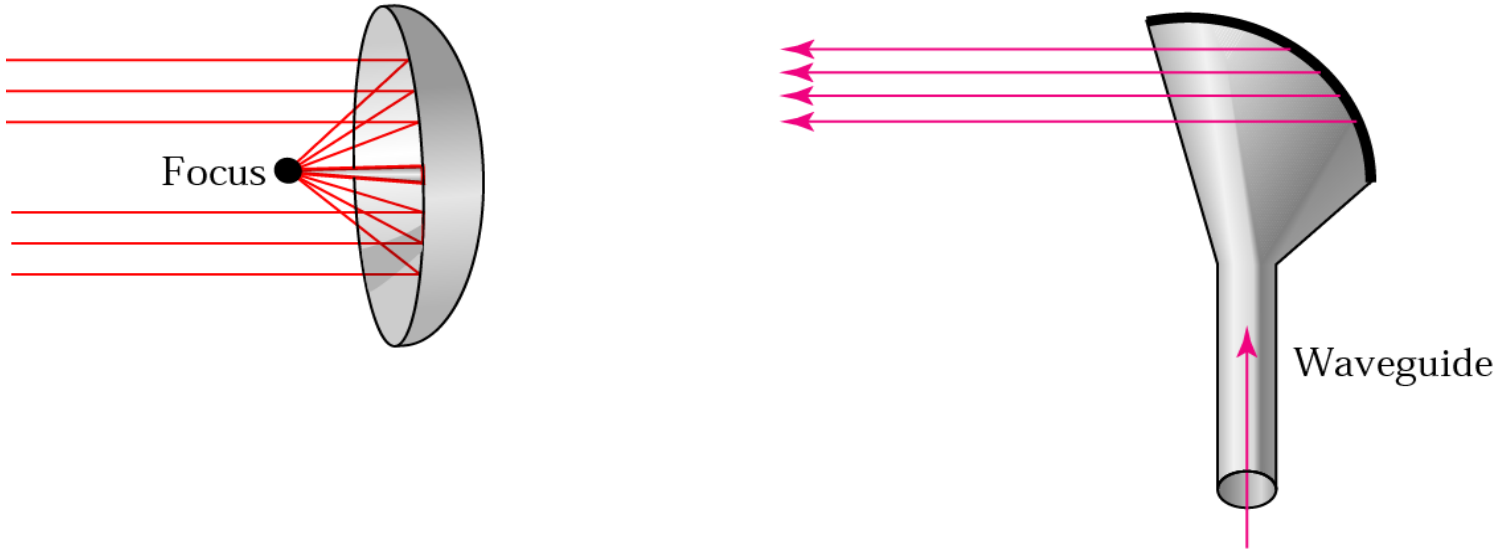
Figure 7.20 *Omnidirectional antennas*





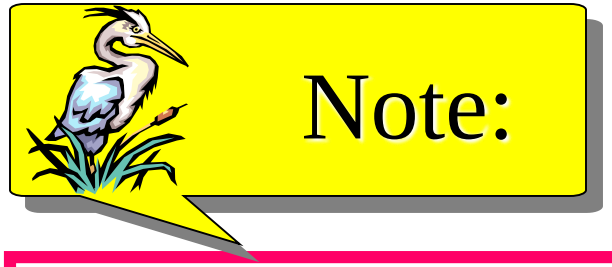
Radio waves are used for multicast communications, such as radio and television, and paging systems.

Figure 7.21 *Unidirectional antennas*



a. Dish antenna

b. Horn antenna



Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Note:

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Signal Propagation Frequencies

Electrical signals are transmitted by converting them into electromagnetic radiation. These radiations are transmitted via antennae that radiate electromagnetic signals. There are various frequency bands within the electromagnetic spectrum and all have different transmission requirements. Figure 1.2 shows the YHF and UHF frequencies for wireless transmission and their transmission properties. Frequency, f, in MHz and wavelength, λ, in meters of electromagnetic radiation are related by the classical formula

$$f = c/\lambda = (300/\lambda) \qquad (1.1)$$

Here the velocity of signal propagation, c, is 300 X 10^6 m/s (this is the velocity of electromagnetic waves in vacuum or air; for other media, such as water, this velocity will be different).

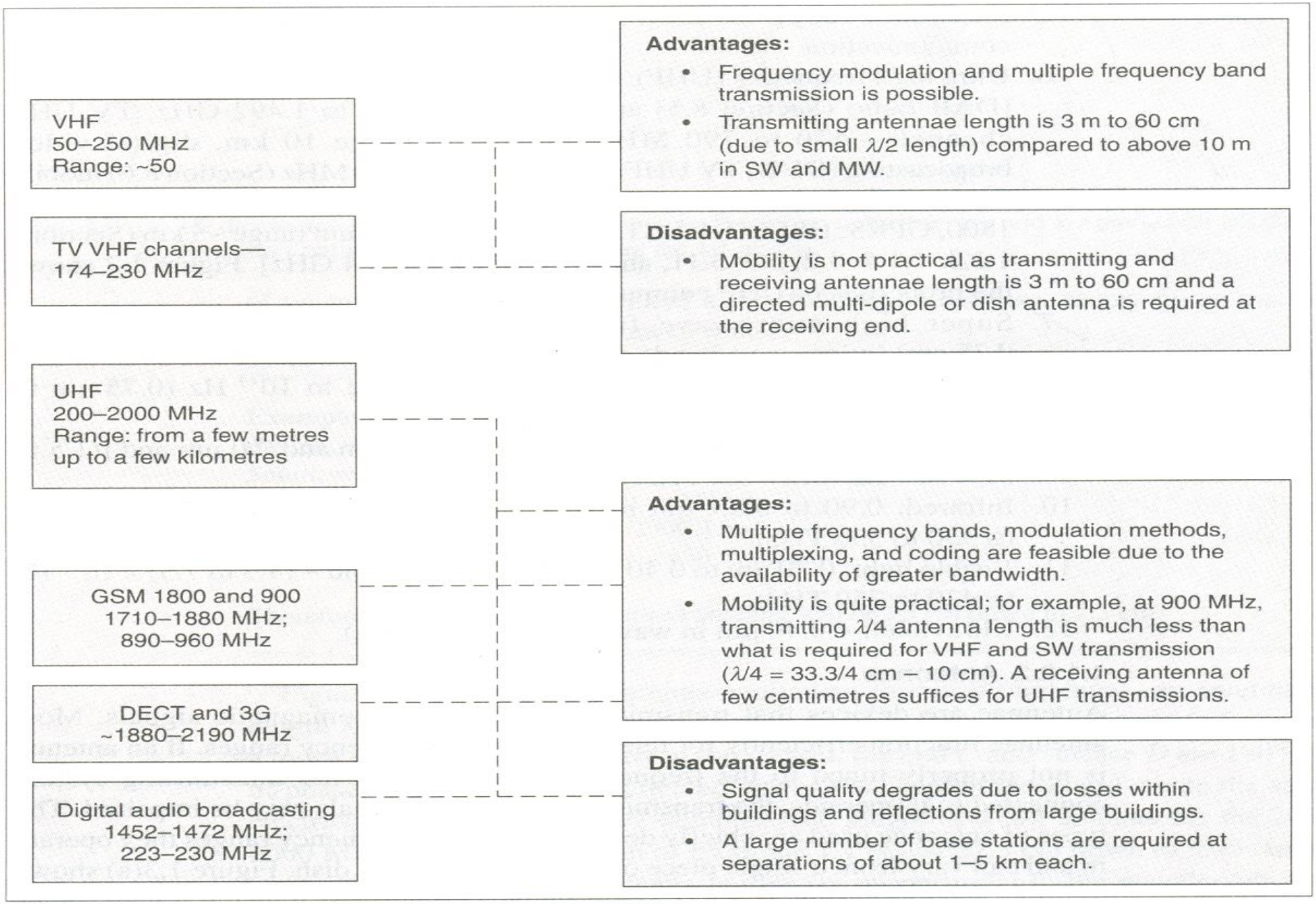
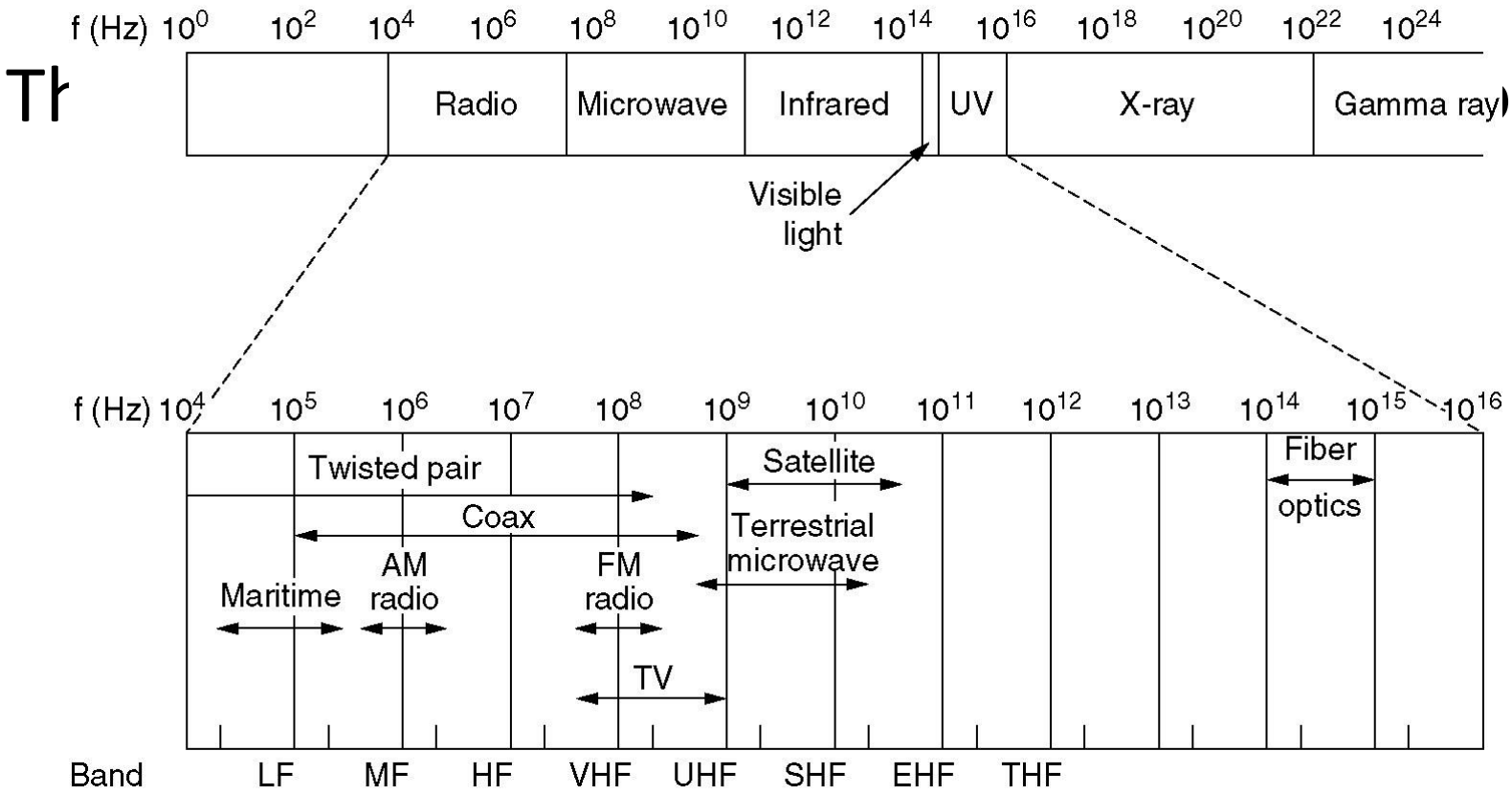
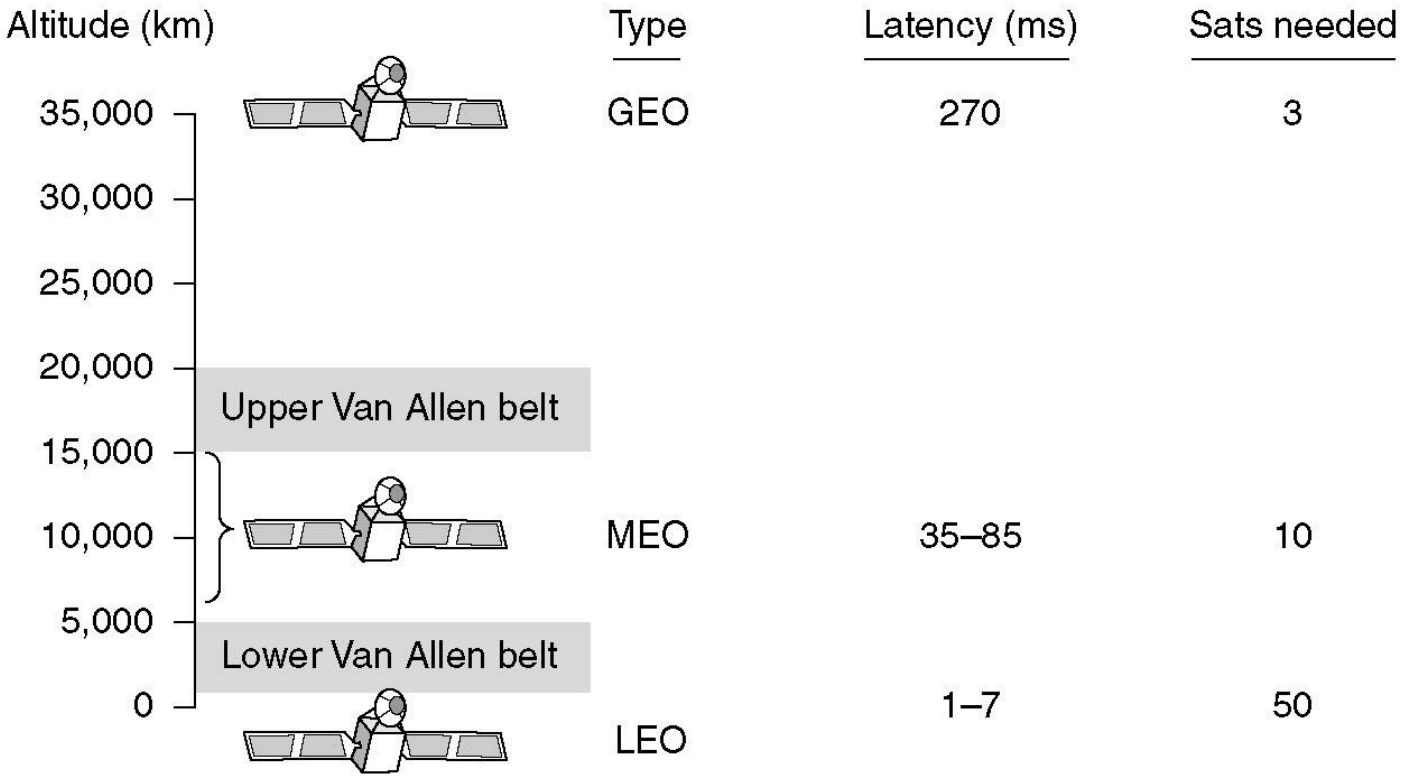


Fig. 1.2 Wireless transmission in VHF and UHF ranges: frequencies and properties

The Electromagnetic Spectrum



Communication Satellites



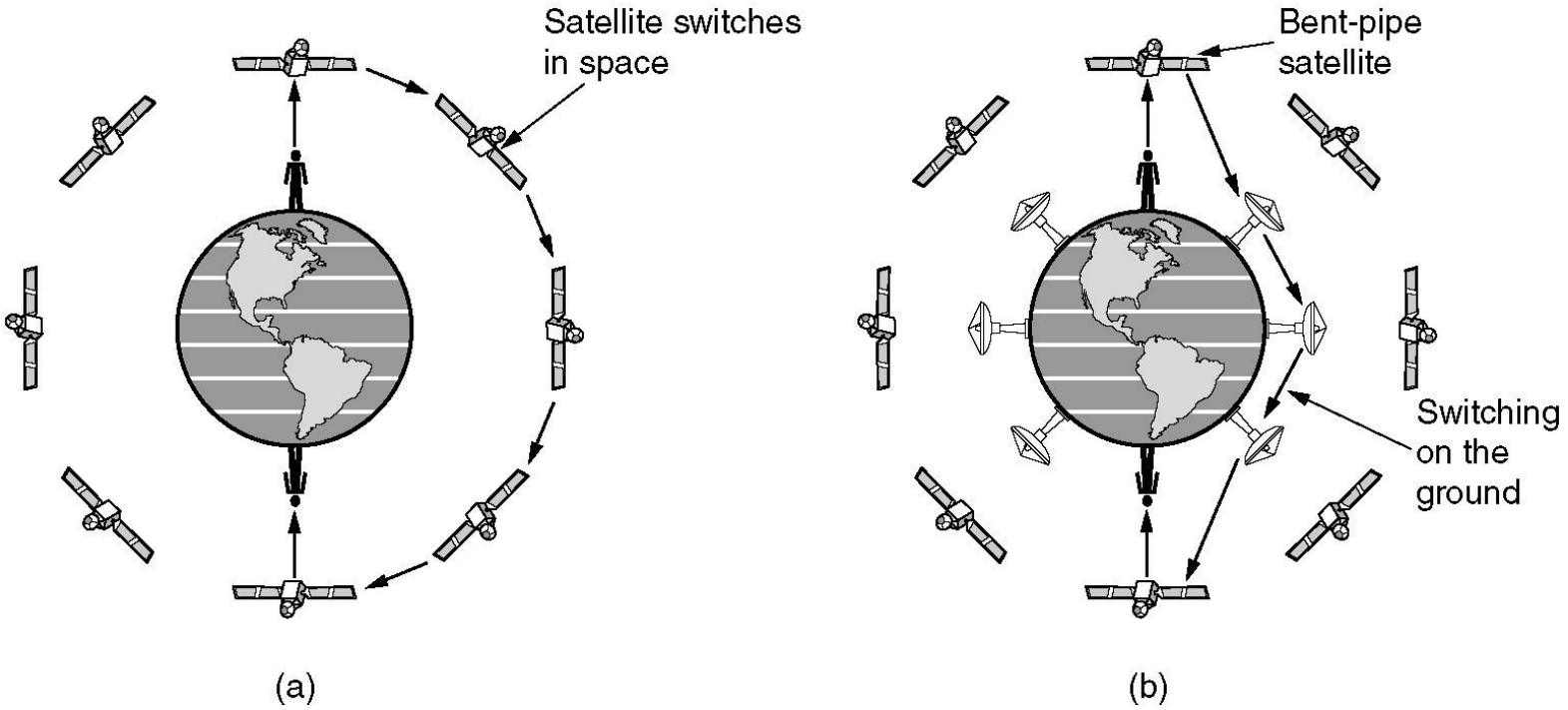
Communication satellites and some of their properties, including altitude above the earth, round-trip delay time and number of satellites needed for global coverage.

Communication Satellites

The principal satellite bands.

Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

Globalstar



(a) Relaying in space.
(b) Relaying on the ground.

The frequencies, and thus wavelengths, of transmitters for various ranges are as follows:

1. Long-wavelength radio, very low frequency (LW): 30kHz to 1 MHz (10,000 to 300 m).
2. Medium-wavelength radio, medium frequency (MW): 0.5 to 2 MHz (600 to 150 m).
3. Short-wavelength radio, high frequency (SW): 6 to 30 MHz (50 to 10 m).
4. FM radio band frequency (FM): 87.5 to 108 MHz (3.4 to 2.8 m), maximum range 50km .
5. Very high frequency (VHF): 50 to 250 MHz (6 to 1.2 m) [digital audio broadcasting (DAB) band III VHF 174 to 240 MHz (Section 8.5), 226 ± 4 MHz, maximum range 50 km, TV VHF channels-174 to 230 MHz, maximum range 50 km]. Figure 1.2 shows the properties of VHF communication.
6. Ultra high frequency (UHF): 200 to ~ 2000 MHz (≡ 2 GHz) (1.5 to 0.15 m) [DAB radio (Section 8.5) at frequencies 1.452 to 1.492 GHz, TV UHF channels- 470 to 790 MHz, maximum range 10 km, digital video broadcasting (DVB) TV UHF Band IV/V470-830 MHz (Section 8.6) mobile TV band IV, 554 MHz, mobile communication frequencies GSM 900, GSM 1800, GPRS, HSCSD, DECT, 3G CDMA, maximum range ~ 5 km (Sections 1.1.3, 1.1.4,3.2,3.9-3.11, and 4.2), Bluetooth 2.4 GHz]. Figure 1.2 shows the properties of UHF communication.
7. Super high microwave frequency (SHF): 2 to 40 GHz (~15 to 0.75 cm) (microwave bands and satellite signal bands).
8. Extreme high frequency (EHF): Above 40 GHz to 10^{14} Hz (0.75 cm to 3μm).
9. Far infrared: Optical wavelengths between 1.0 urn and 2.0 urn and [(1.5 to 3) x 10^{14} Hz (0.15-0.3 THz)].
10. Infrared: 0.90 to 0.85 urn in wavelength and ~ (3.3 to 3.5) x 10^{14} Hz (≡ 350 to 330 THz).
11. Visible light: 0.70 urn to 0.40 urn in wavelength and ~ (4.3 to 7.5) x 10^{14} Hz (= 430 to 750 THz).
12. Ultraviolet: < 0.40 μn in wavelength (> 750 THz).

IEEE 802 Standards

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

The 802 working groups. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.

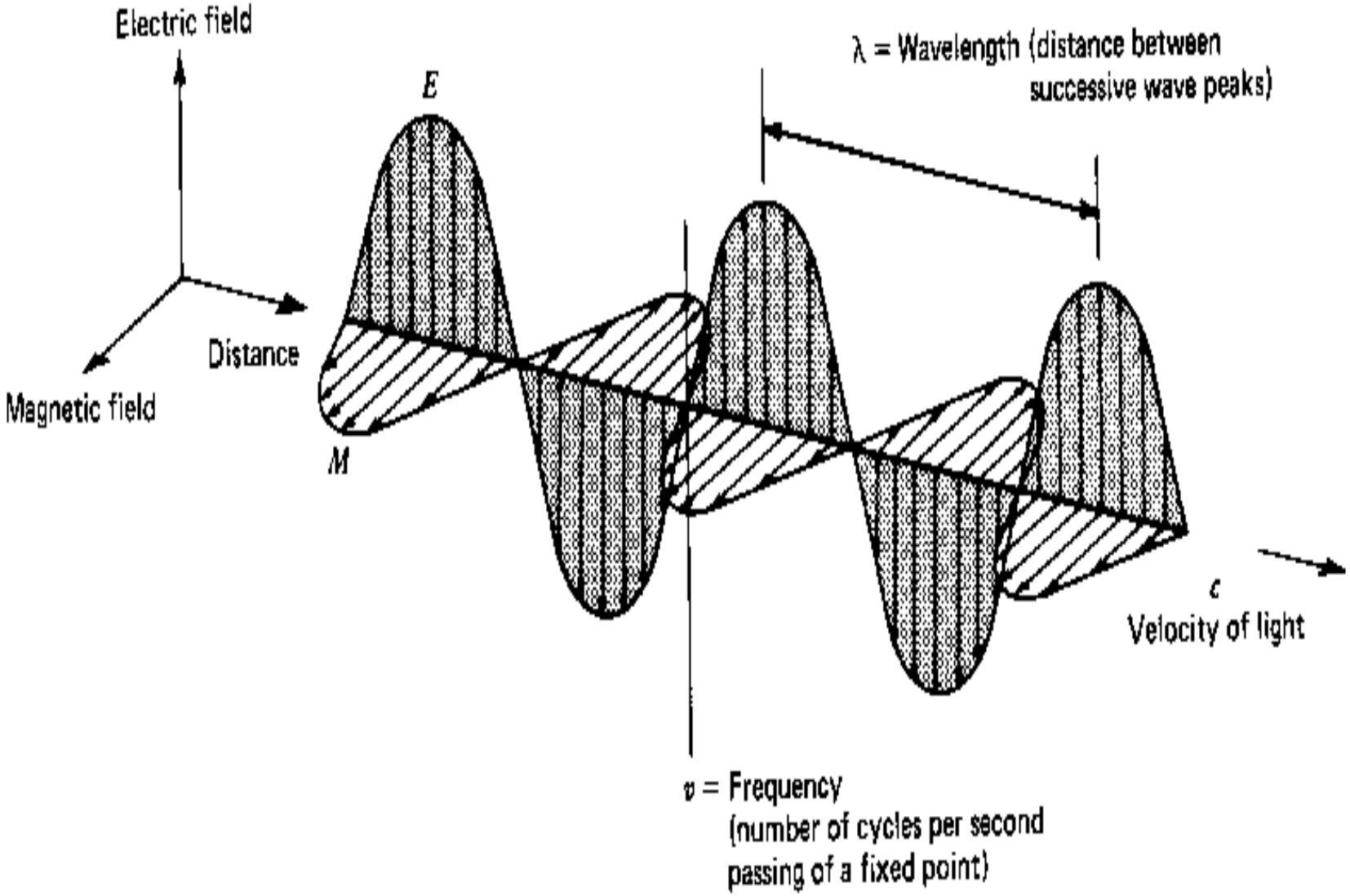
Antennae

Antennae are devices that transmit and receive electromagnetic signals. Most antennae function efficiently for relatively narrow frequency ranges. If an antenna is not properly tuned to the frequency band in which the transmitting system connected to it operates, the transmitted or received signals may be impaired. The types of antennae used are chiefly determined by the frequency ranges they operate in and can vary from a single piece of wire to a parabolic dish. Figure 1.3(a) shows a simple antenna design. It is a λ/2-long antenna for wireless transmission of waves

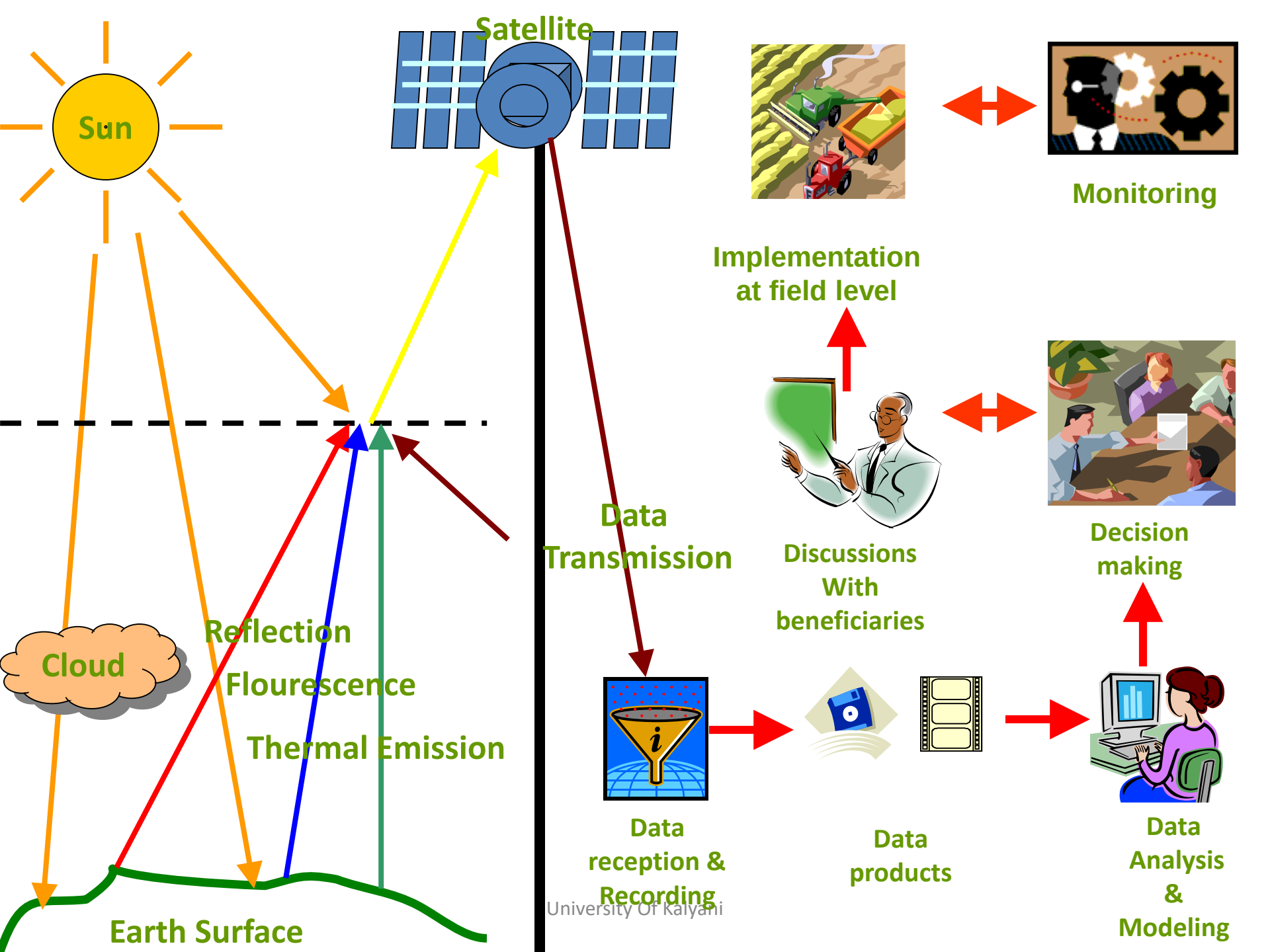
Defn. of Antena

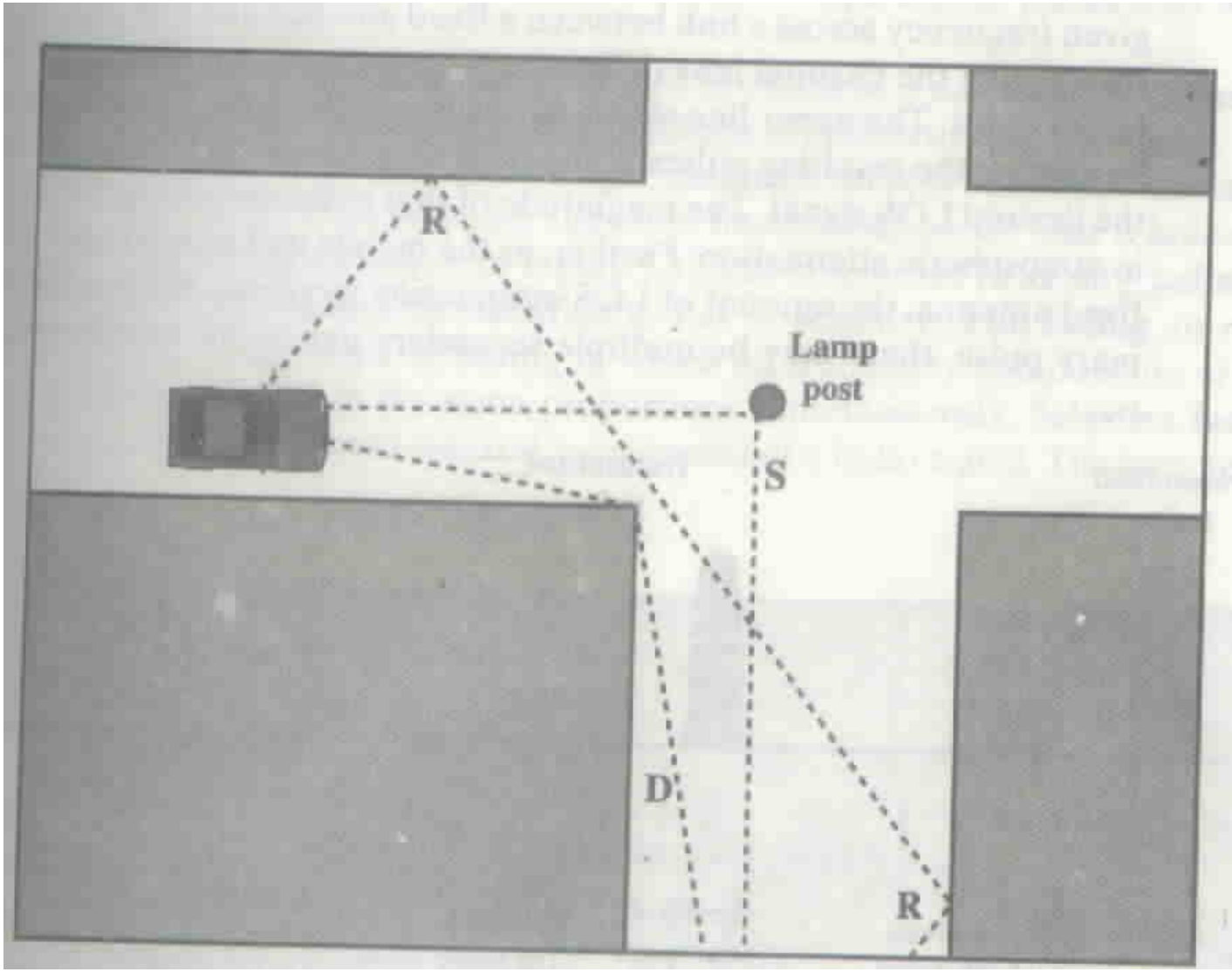
Antenna is an electrical conductor or system of conductors used for radiating electromagnetic energy into space or for collecting electromagnetic energy from the space

– An integral part of a wireless system

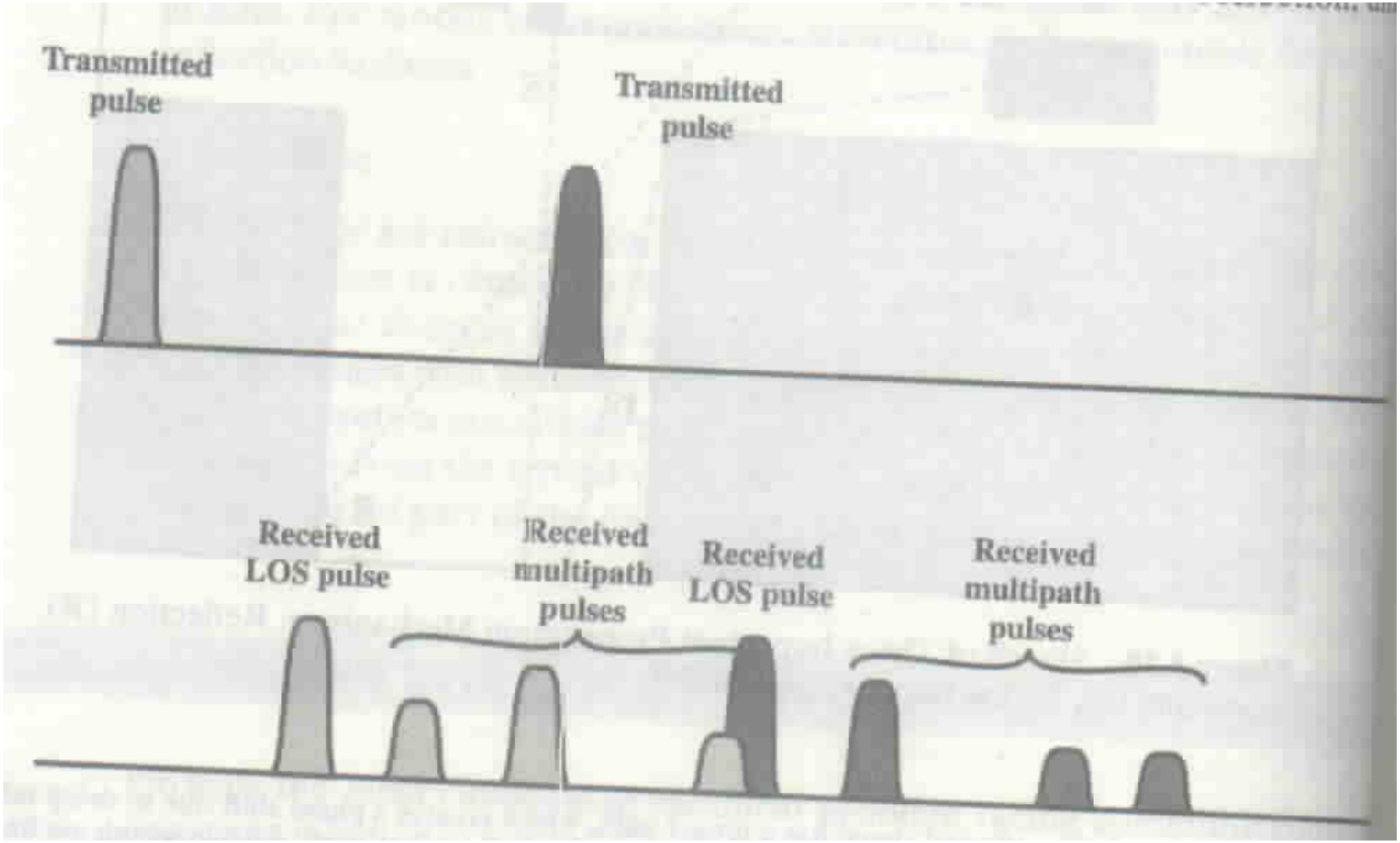


An electromagnetic wave. Components include a sinusoidal electric wave (E) and a similar magnetic wave (M) at right angles, both being perpendicular to the direction of propagation.


Satellite
Sun
Monitoring
Implementation at field level
Data Transmission
Discussions With beneficiaries
Decision making
Cloud
Reflection
Flourescence
Thermal Emission
Data reception & Recording
Data products
Data Analysis & Modeling
Earth Surface



Multipath Propagation



Inter Symbol Interference (ISI) in multipath

Effect of Multipath Propagation

- Multiple copies of the signal may arrive with different phases. If the phases add destructively, the signal level reduces relative to noise.
- Inter Symbol Interference (ISI)

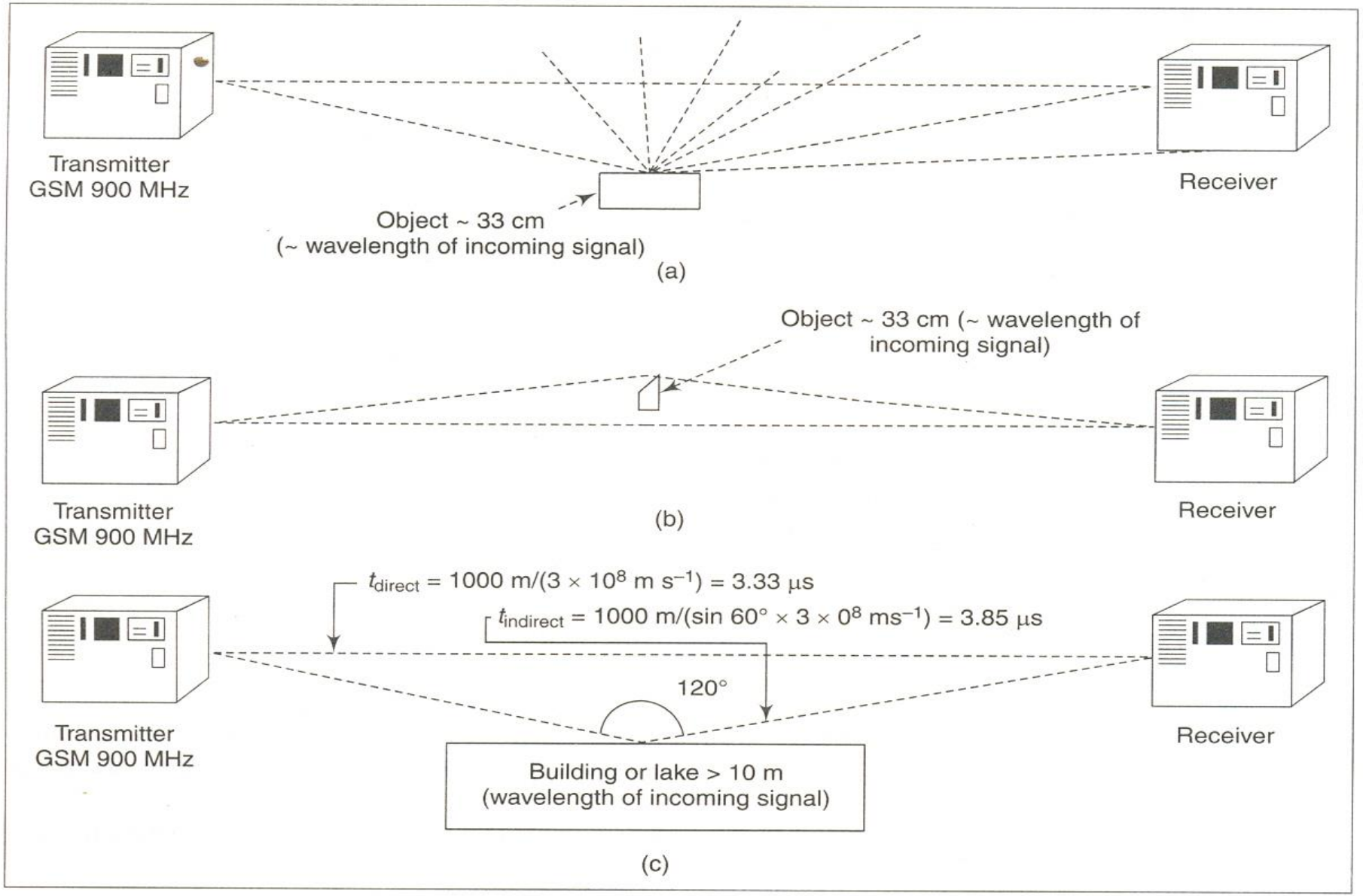


Fig. 1.5 (a) Scattering of signal (b) Diffraction of signal (c) Reflected and direct signals from a 900 MHz transmitter and calculation of delay

(e) The signal may also be *reflected* from the surface of an obstacle, the earth's surface, or a water body of size greater than the wavelength of the signal. For example, if a transmitter sends out a GSM 900 MHz (A = 33 cm) signal, then the transmitter signal reflects from an object of size 10 m and above (much greater than A) .The reflected signal suffers a delay in reaching its destination. Figure l.5(c) shows the reflection and the delay. The delay is more pronounced in case of multi-hop paths. Delayed signals have distorted waveforms and cause misrepresentation of information encoded in the signal. There are digital signal processing techniques to eliminate the distortions due to delays from direct and multiple paths so that the original signal can be recovered. The delay in the reflected signal with respect to the original direct signal is given as .

$$\text{Delay} = t_{\text{indirect}} - t_{\text{direct}} = \frac{\text{additional path travelled in meters}}{3 \times 10^8 \,\text{m s}^{-1}} \qquad (1.2)$$

Example 1.4 A receiver receives two signals, one directly in line-of-sight and the other after a reflection of 120° from a transmitter at a distance of 1000 m (Fig. 1.5(c)). Calculate the delay in the reflected signal with respect to the direct signal.

Solution: Direct path time, $t_{direct} = \dfrac{1000\ \text{m}}{3 \times 10^8\ \text{ms}^{-1}} = 3.33\ \mu\text{s}$

Reflected path time, $t_{indirect} = \dfrac{1000\ \text{m}}{\sin(120°/2) \times (3 \times 10^8\ \text{ms}^{-1})} = 3.85\ \mu\text{s}$

Delay in reflected signal with respect to direct signal $= t_{indirect} - t_{direct}$
$= 3.85–3.33\ \mu\text{s} = 0.52\ \mu\text{s}$

Figure 4.22 *From analog signal to PCM digital code*

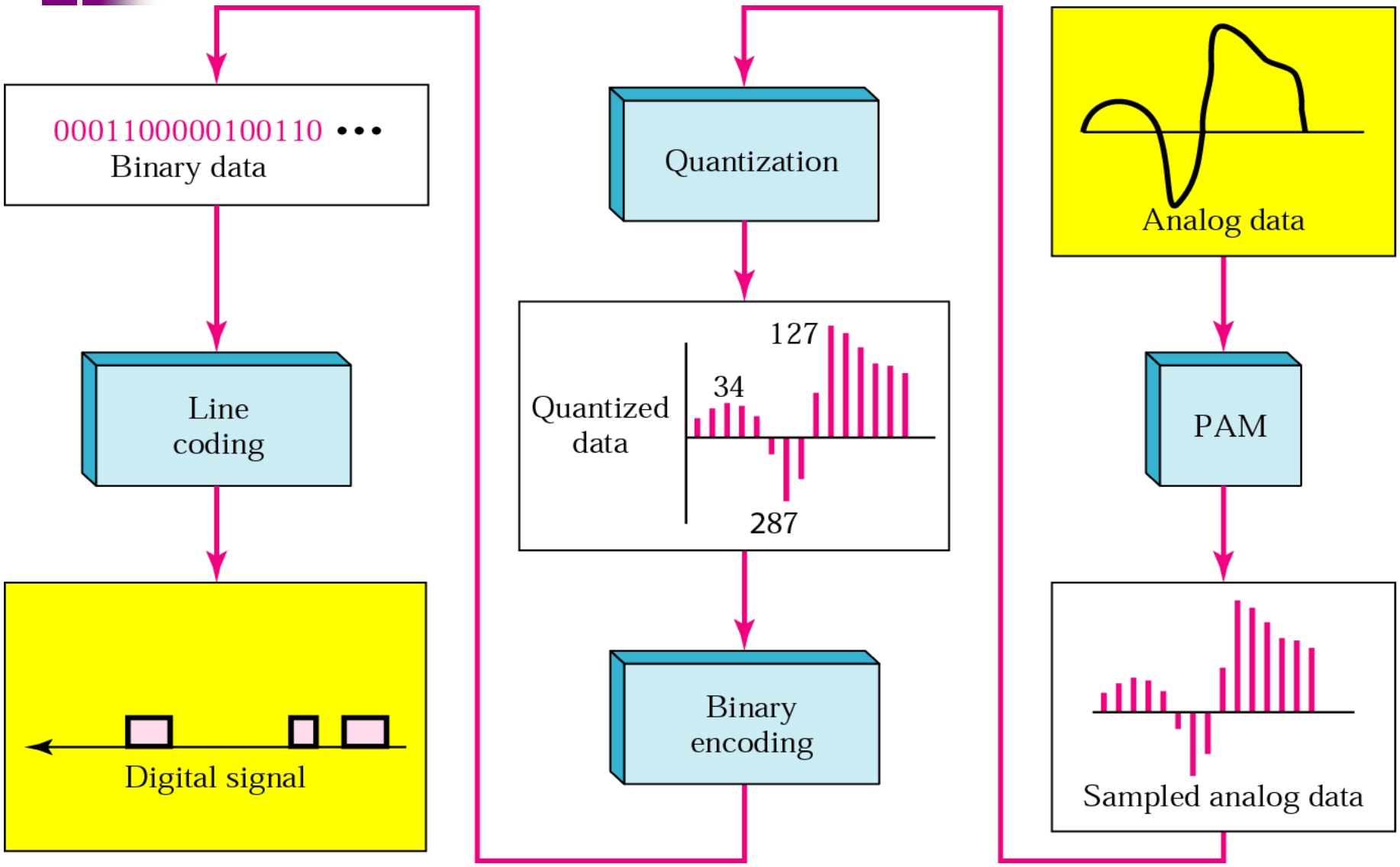


Figure 5.3 *ASK*

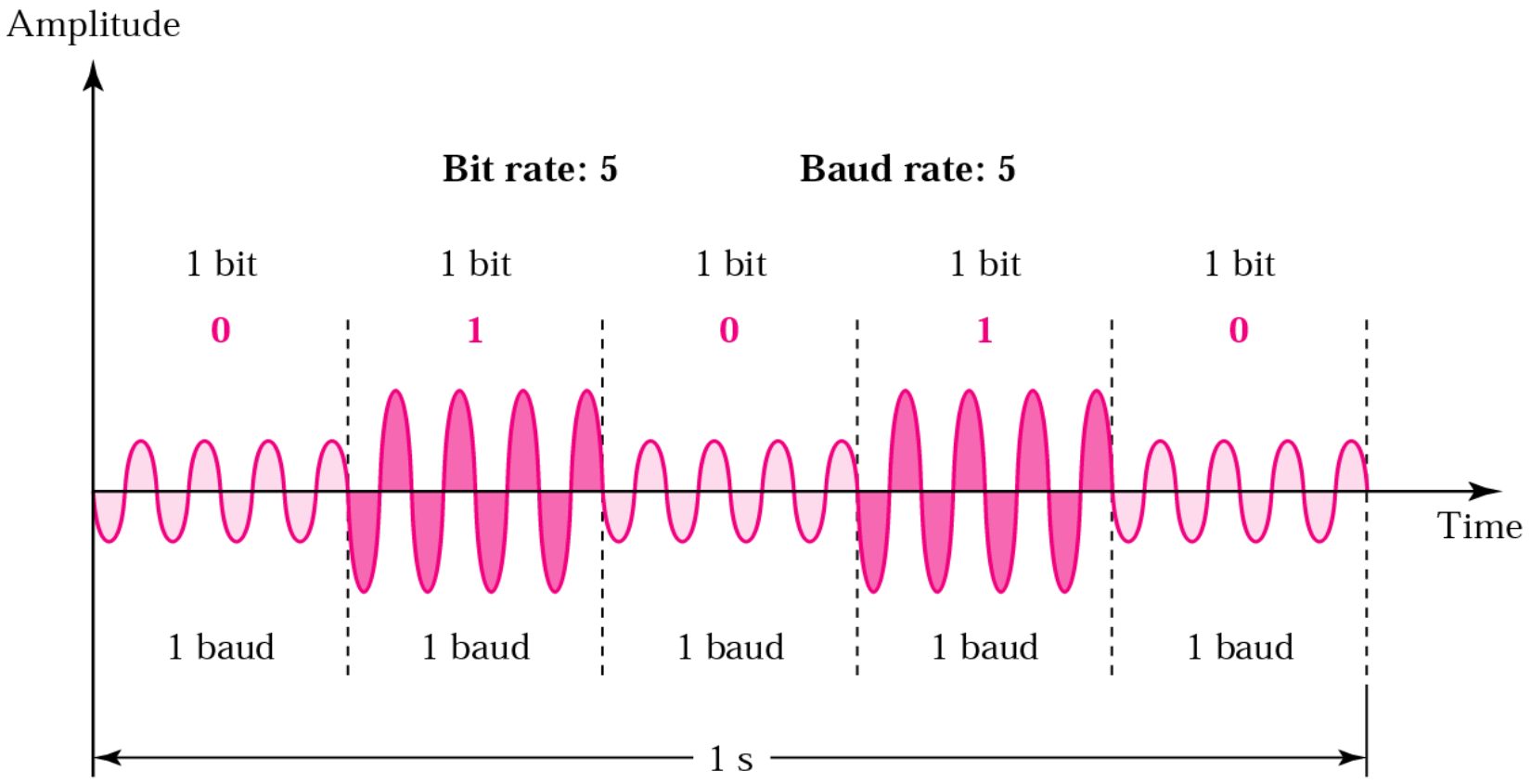


Figure 5.6 *FSK*

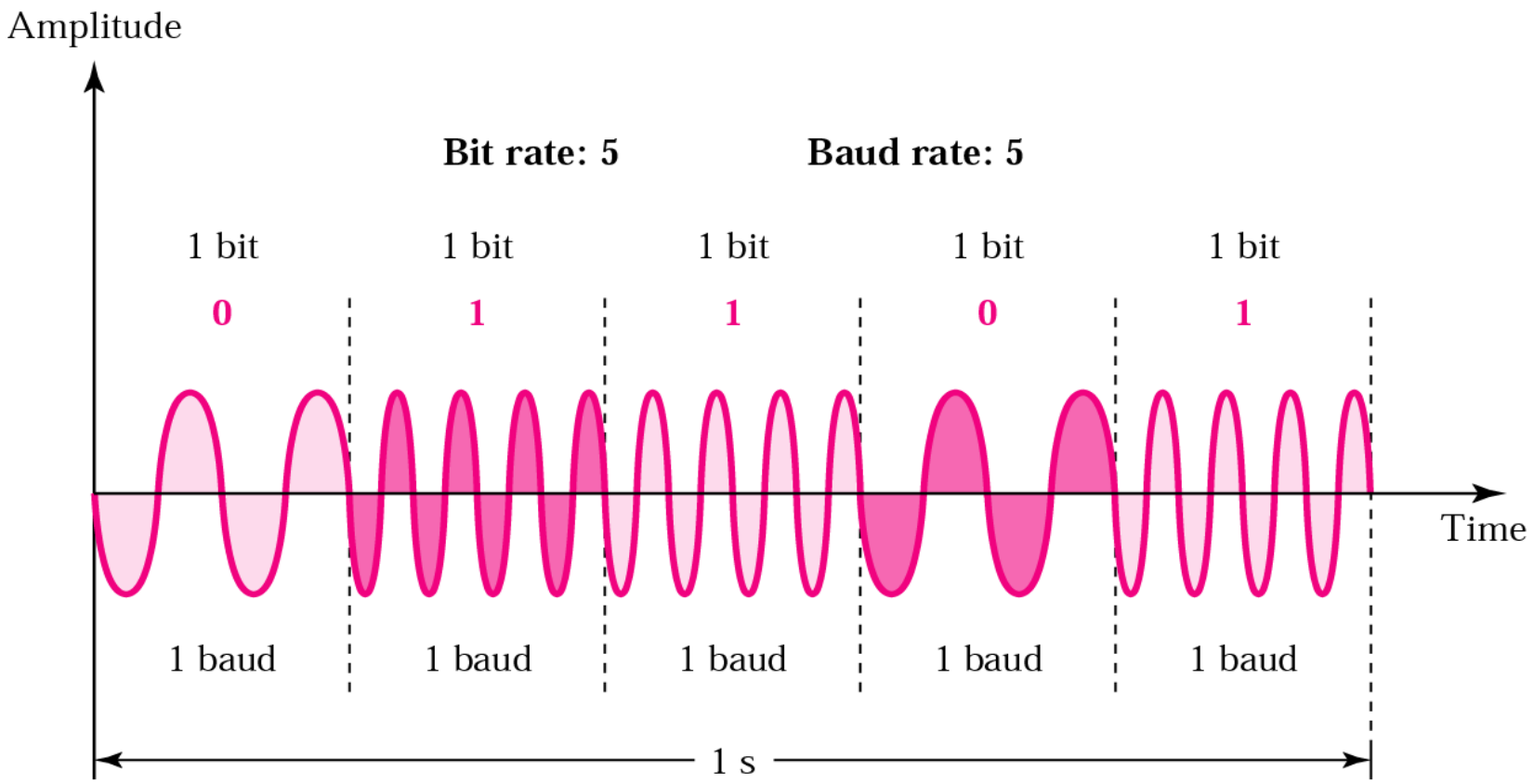


Figure 5.8 *PSK*

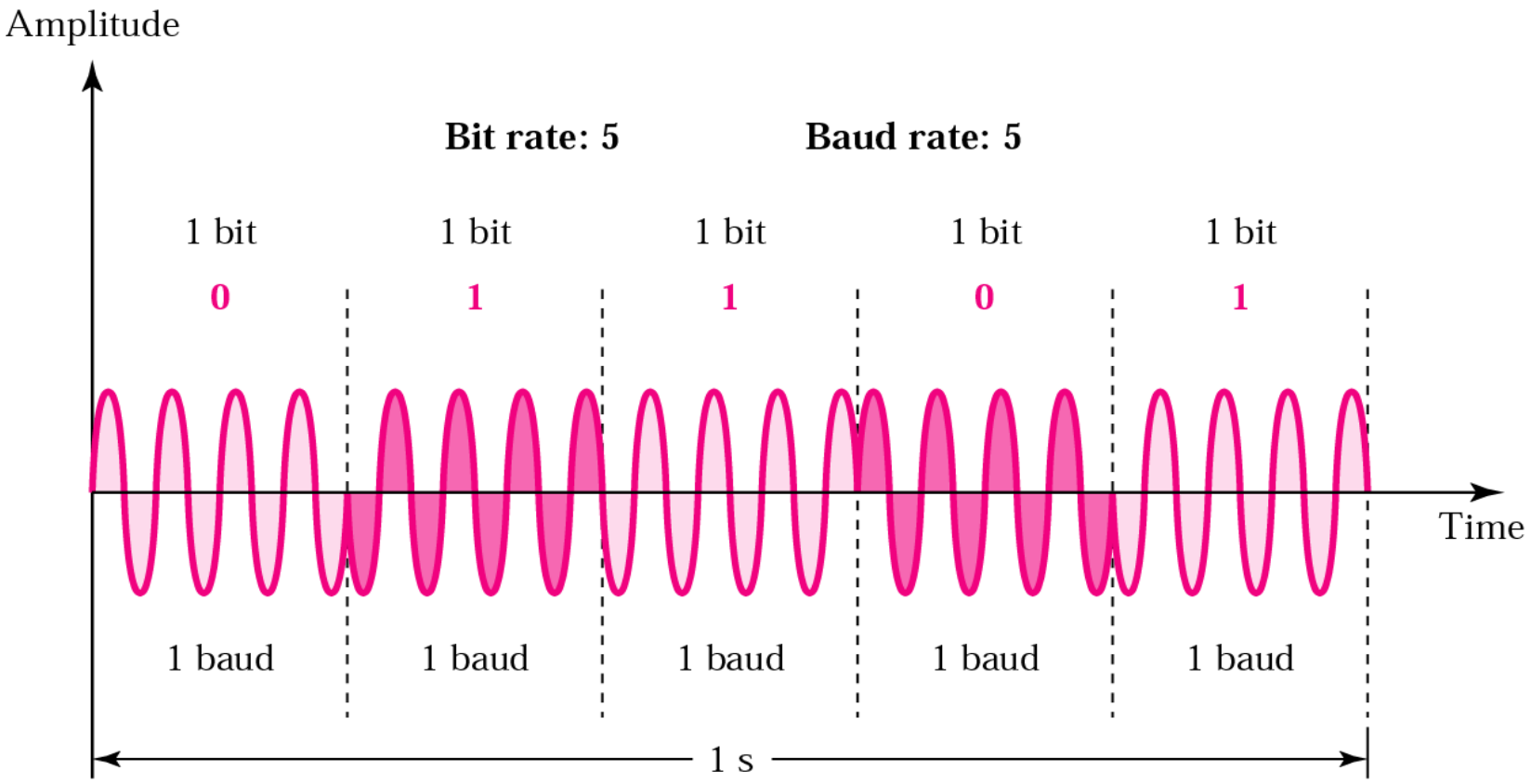


Figure 5.15 *Time domain for an 8-QAM signal*

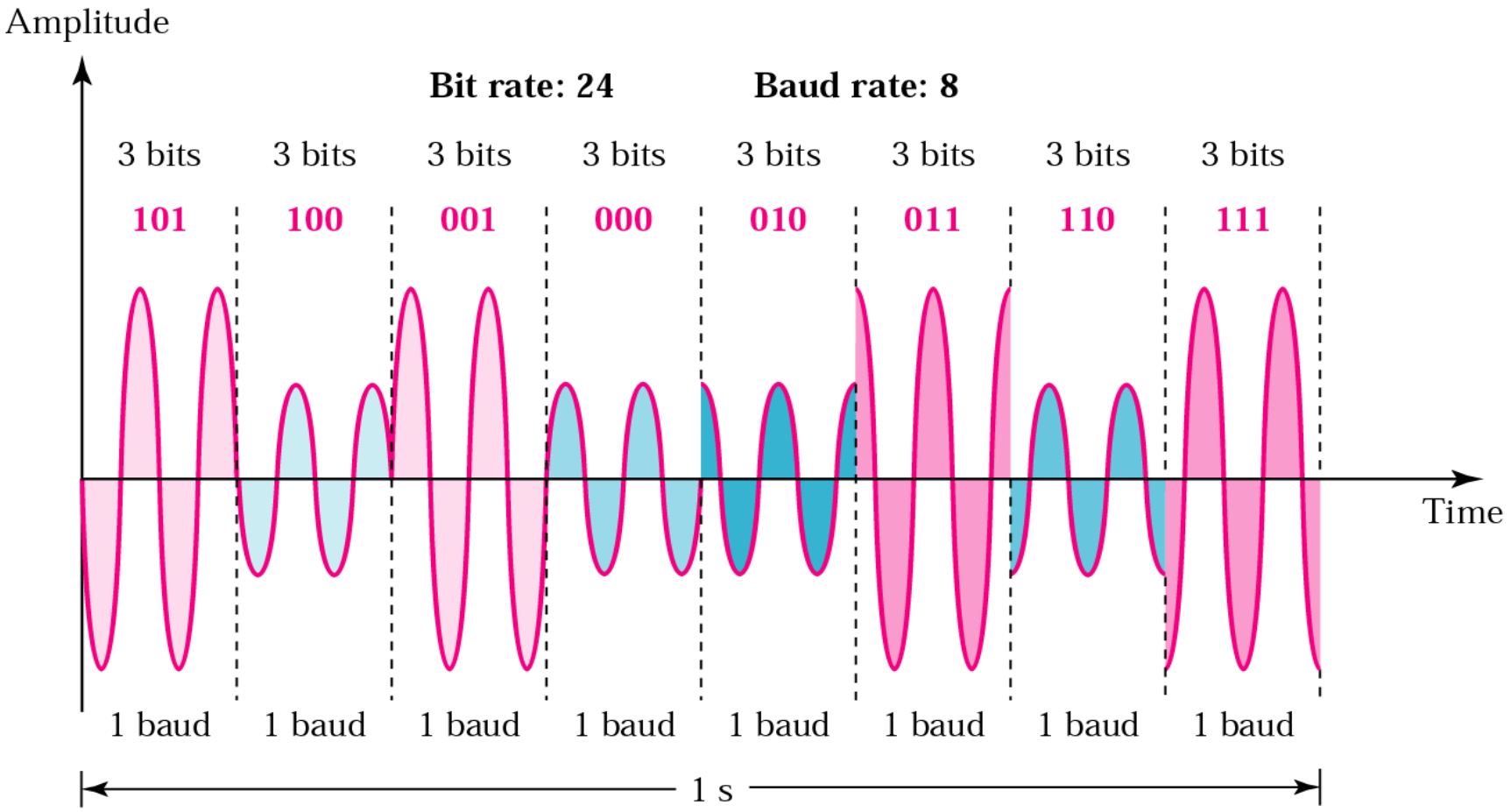


Figure 6.4 *FDM process*

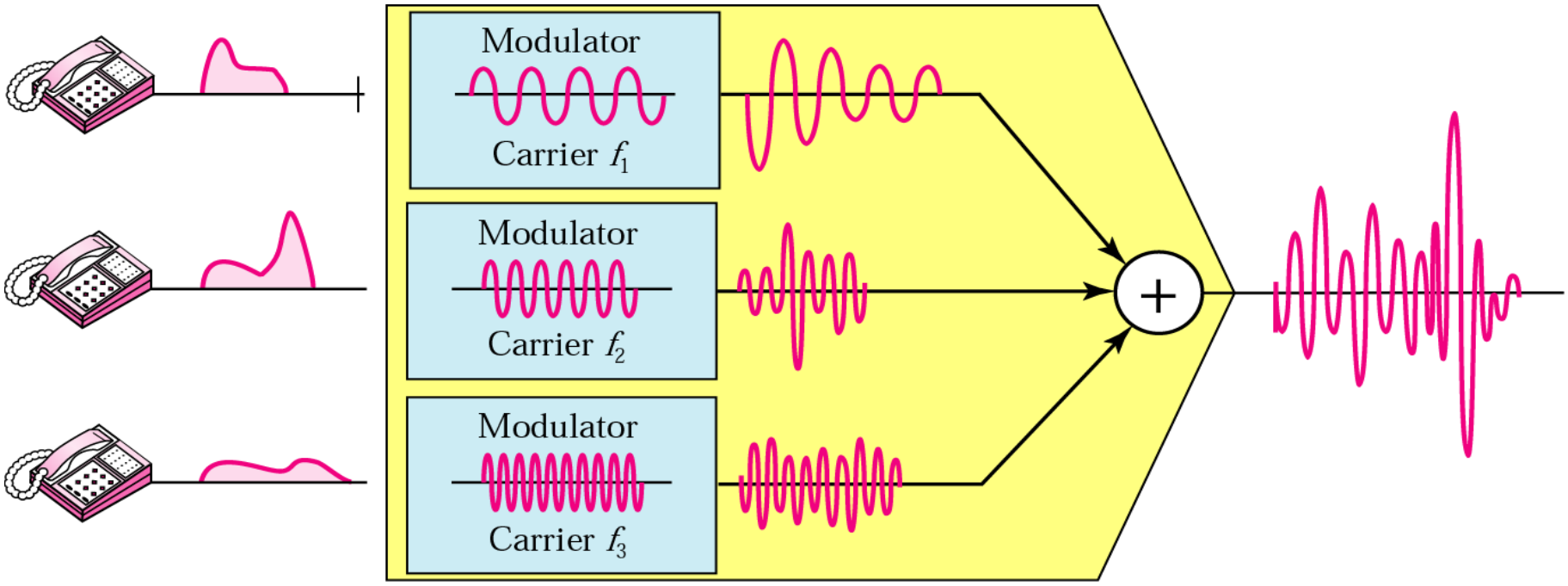
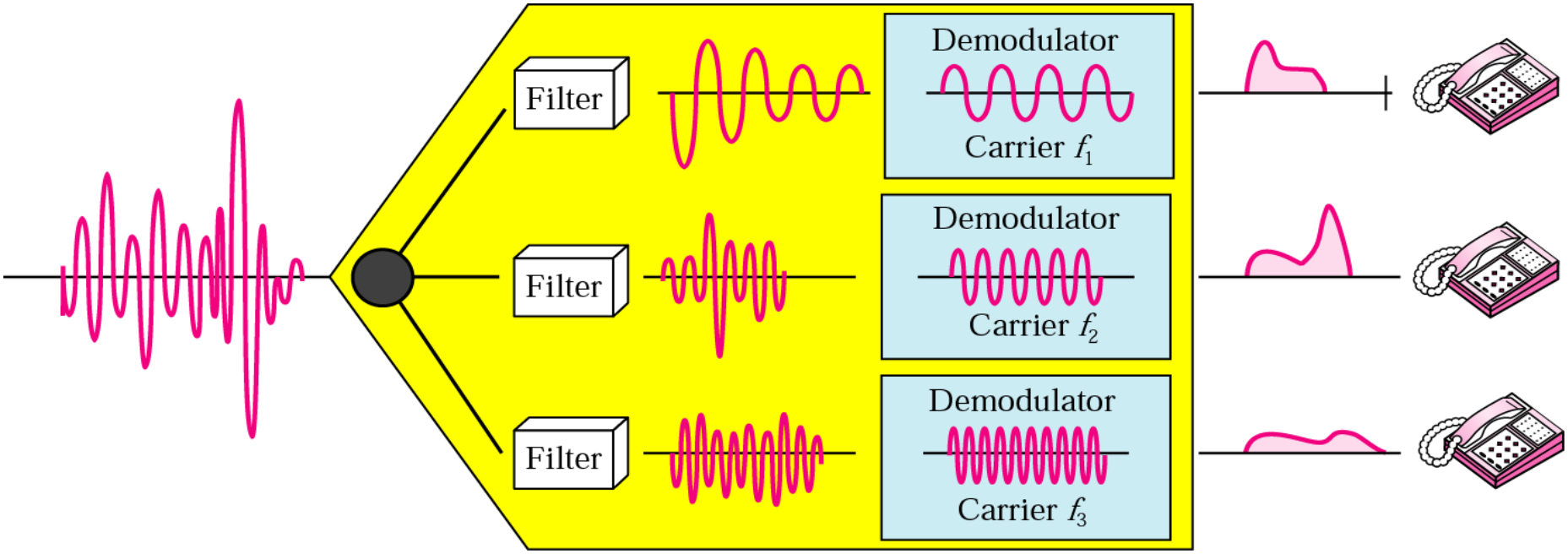


Figure 6.5 *FDM demultiplexing example*



GSM

- The global system for mobile communications (GSM) was developed by the Group Special Mobile (GSM) which was founded in Europe in 1982. The GSM is a standard for mobile telecommunication through a cellular network at data rates of up to 14.4 kbps. Nowadays it consists of a set of standards and protocols for mobile telecommunication. Table 1.2 summarizes the standards based on GSM. Chapter 3 will discuss GSM in detail.

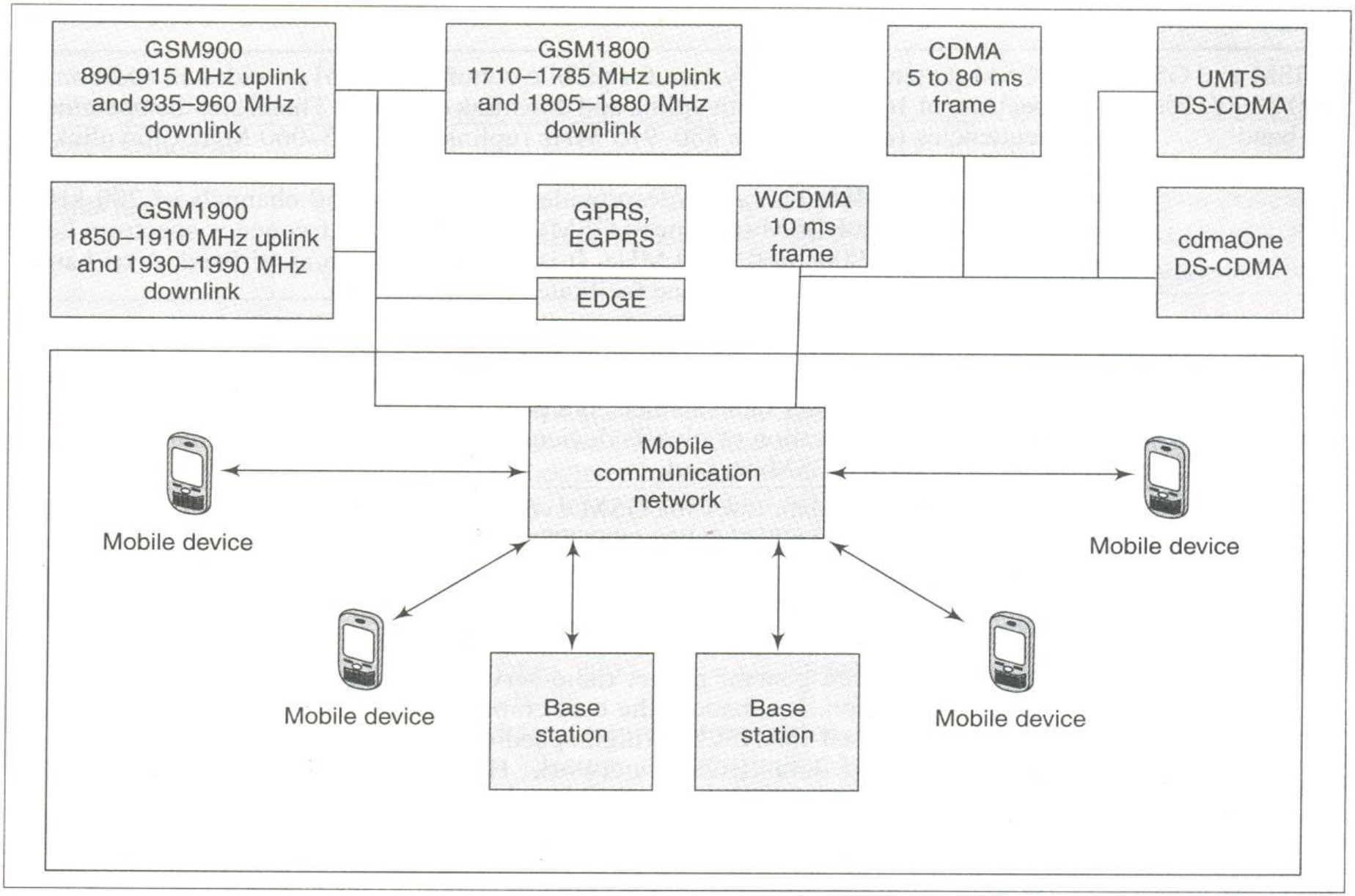
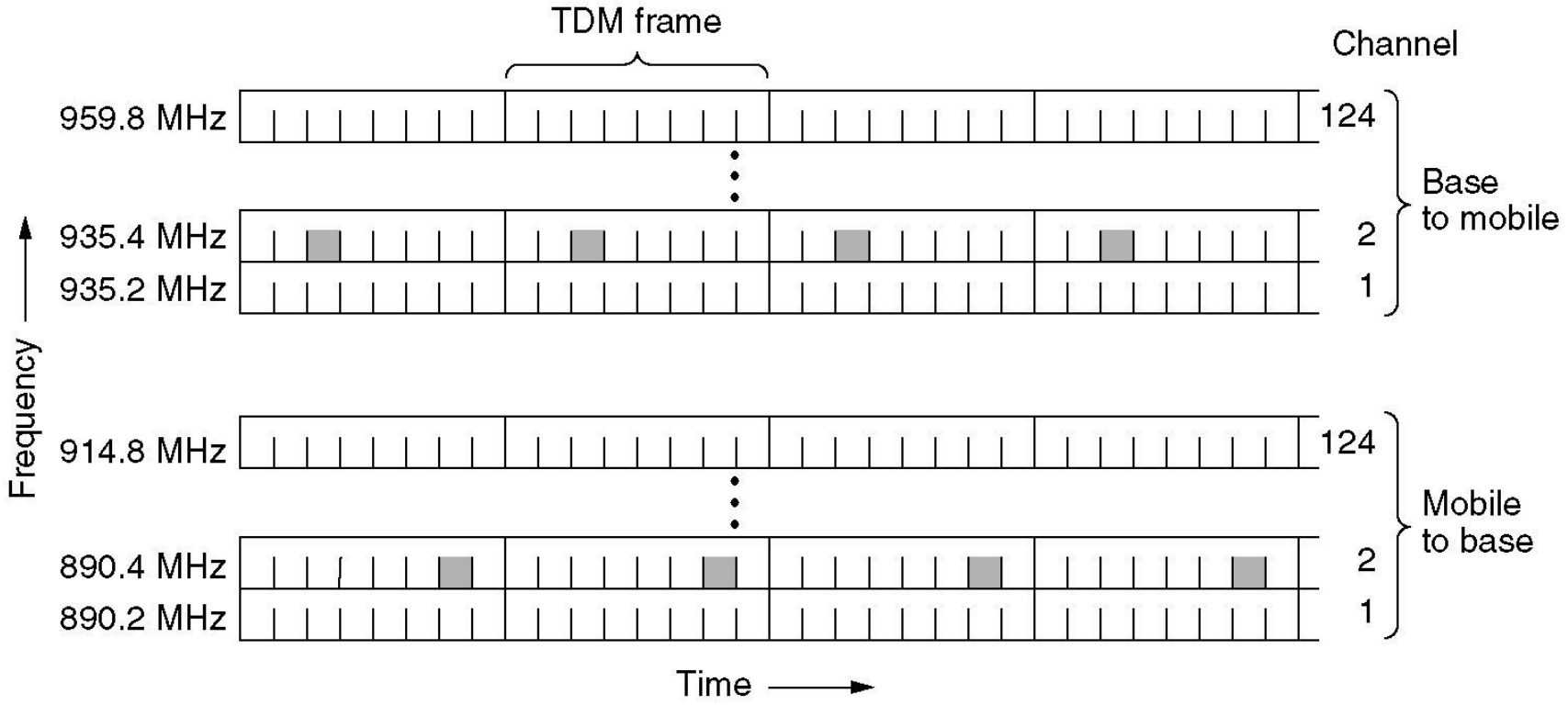


Fig. 1.9 GSM- and CDMA-based standards and a mobile communication network for long distance communication

GSM
Global System for Mobile Communications



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

GSM (2)

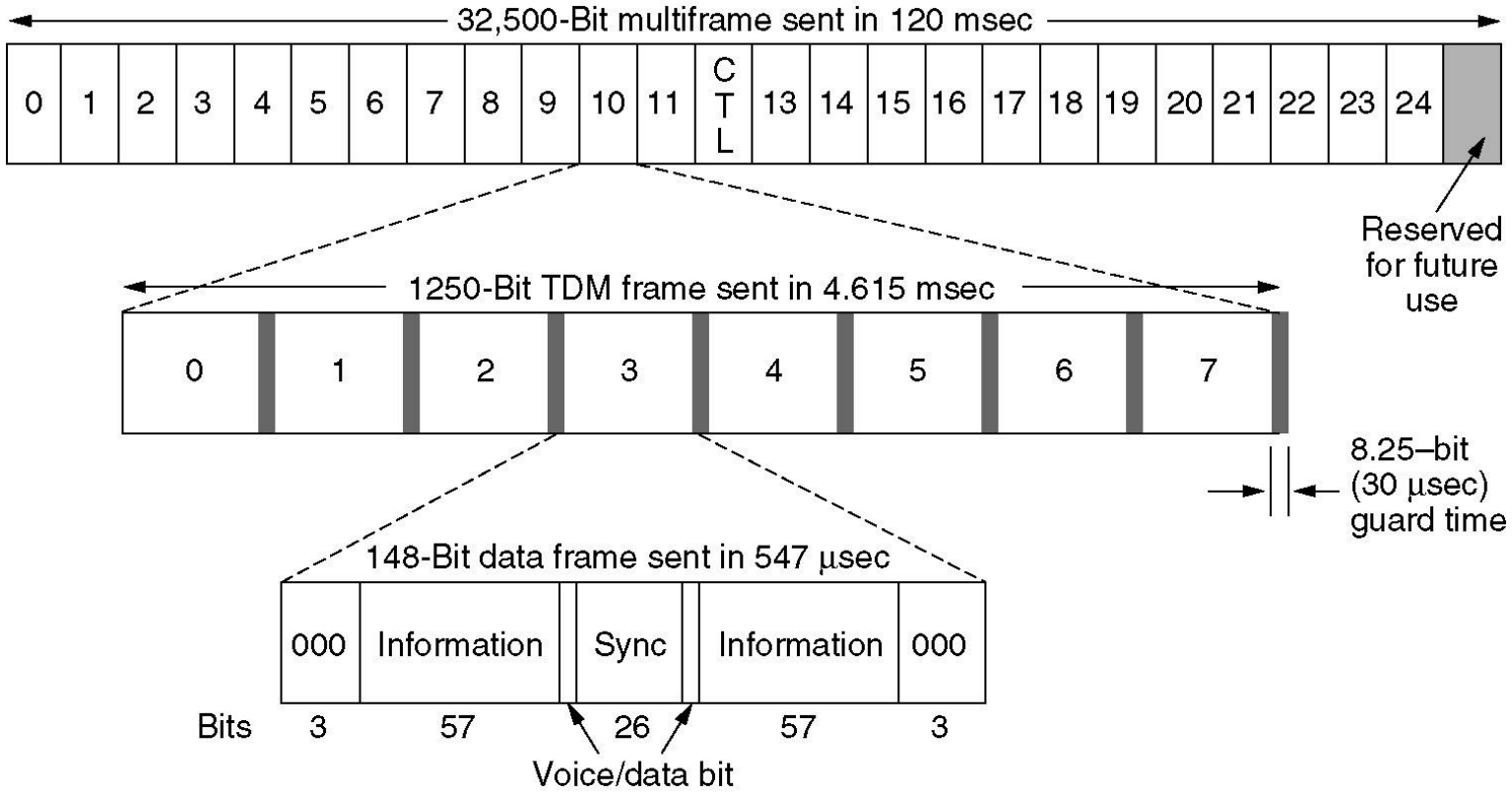

32,500-Bit multiframe sent in 120 msec
0 1 2 3 4 5 6 7 8 9 10 11 CTL 13 14 15 16 17 18 19 20 21 22 23 24
Reserved for future use
1250-Bit TDM frame sent in 4.615 msec
0 1 2 3 4 5 6 7
8.25–bit (30 μsec) guard time
148-Bit data frame sent in 547 μsec
000 Information Sync Information 000
Bits 3 57 26 57 3
Voice/data bit

Table 1.2 Standards based on the GSM

Extension / Enhancement	*Description*
GSM900	The GSM (Groupe Spéciale Mobile) was founded in Europe in 1982. This led to a communication standard being founded in 1988, which is also known as GSM (global system for mobile communications). GSM uses GMSK (Section 1.1.2(4)) for transmitting 1s and 0s. GSM uses FDMA for channels and TDMA for user access in each deployed channel. Up to eight radio-carrier analog signals are transmitted using one common digital channel of bandwidth 200 kHz (Section 1.1.2(5)). GSM900 operates at 890–915 MHz for uplink and 935–960 MHz for downlink. Uplink and downlink frequency bands of 25 MHz each provide FDMA access for each channel. Each link thus provides 124 channels, each of 200 kHz. Each channel provides eight TDMA access slots, thus providing channel access to each user (radio carrier) every 4.615 μs. Users have time-slices of 577 ms each. The data rates of a GSM mobile-communication network are at maximum 14.4 kbps (kilobytes per second).

(*contd*)

(*contd*)

EGSM and GSM 900/1800/1900 tri-band	EGSM (extended global system for mobile communication) provides an additional spectrum of 10 MHz on both uplink and downlink channels. Therefore, the operating frequencies for EGSM are 880–915 MHz (uplink) and 925–960 MHz (downlink). The link frequencies are just below and above the original GSM 900 band. The additional 10 MHz on each side provides an additional 50 channels of 200 kHz each. Nowadays EGSM (enhanced GSM) communication frequency spectrum lies in three bands, 900/1800/1900 MHz. It is therefore known as tri-band. A tri-band radio carrier in the mobile phone facilitates global roaming. GSM 1800 uses 1710–1785 MHz for uplink and 1805–1880 MHz for downlink. GSM 1900 uses 1850–1910 MHz for uplink and 1930–1990 MHz for downlink.
GPRS [GSM Phase2+ (2.5G)]	GPRS (general packet radio service) is a packet-oriented service (Section 1.1.2(6)) for data communication of mobile devices and utilises the unused channels in the TDMA mode in a GSM network.
EDGE	EDGE (enhanced data rates for GSM evolution) is an enhancement of the GSM Phase 2 [known as GSM Phase 2.5G+]. It uses 8-PSK (Section 1.1.2(4)) communication to achieve higher rates of up to 48 kbps per 200 kHz channel as compared to the up to 14.4 kbps data transmission speed in GSM. Using coding techniques the rate can be enhanced to 384 kbps for the same 200 kHz channel.
EGPRS	EGPRS (enhanced general packet radio service) is an extension of GPRS using 8-PSK modulation. It enhances the data communication rate. EGPRS is based on EDGE and is used for HSCSD (high-speed circuit-switched data)—an enhanced circuit-switched data (ECSD) network. HSCSD is a GSM Phase2+ (2.5G) communication standard. For example, the Nokia 9300 Series Smartphone has high-speed data connectivity with EGPRS (EDGE), mobile Internet connectivity and tri-band (EGSM 900/1800/1900) operation for use in all five continents.

CDMA

- Besides GSM, CDMA is the most popular mobile communication standard (Fig. 1.9). The initial evolution of CDMA was as 2.5G. It started in 1991 as cdma One (IS-95). Nowadays CDMA supports high data rates and is considered 3G. CDMA devices transmit voice as well as data and multimedia streams. CDMA 2000, IMT- 2000, WCDMA, and UMTS, like the GSM, also support cellular networks (Section 1.5.1). Table 1.3 summarizes the standards based on CDMA. Sections 4.2-4.7 will describe CDMA standards in detail.

Wireless Personal Area Network

- The previous section dealt with the long distance wireless mobile network communication standards GSM and CDMA. A wireless personal area network (WPAN) enables wireless communication between devices that are at short distances from each other. Figure 1.10 shows a wireless-based personal area network. It facilitates communication of mobile devices with home computers and with other devices at short distances.

Table 1.3 CDMA based standards

Extension / Enhancement	*Description*
2.5G+ standards	
cdmaOne/IS-95	CdmaOne founded in 1991, developed by QUALCOM, USA, belongs to 2G+, also known as IS-95 (interim standards 95). IS-95 operates at 824–849 MHz and 869–894 MHz. A CDMA channel can transmit analog signals from multiple sources and users.
3G standards	
3GPP (WCDMA)	The 3GPP (3G partnership project), also known as WCDMA (Wide CDMA), supports asynchronous operations and has a 10 ms frame length with 15 slices. It has a smaller end-to-end delay in the 10 ms frame as compared to 20, 40, or 80 ms frames. Each frame length is modulated by QPSK both for uplink and downlink. It uses DS (direct sequence) CDMA. It supports a 3.84 Mbps chipping rate (Section 4.3). Both short and long scrambling codes are supported, but for uplink only.
3GPP2 (IMT-2000, CDMA 2000)	3GPP2 (3G partnership project 2) started in 2001. It is compatible with CDMA 2000 and CDMA 2000 1x. The 3GPP2 chipping rates are in multiples of f_s = 1.2288 Mbps. 3G IMT 2000 carrier frequency f_{c0} = 2 GHz (Section 1.2.6). This is included in UMTS. The CDMA 2000 1x f_s = 1.2288 Mbps and is also backward compatible to 2.5G cdmaOne IS-95. 3GPP2 is used for voice communication, for circuit as well as packet-switched communication (Section 1.1.2.6), internet protocol (IP) packet transmission, and multimedia and real-time multimedia applications. It supports higher data rates, synchronous operations, and 5, 10, 20, 40, or 80 ms frame length. Each frame length is modulated by QPSK and BPSK—for uplink and down link, respectively. CDMA 2000 1x EVDO (evolution for data optimized) and CDMA 2000 1x EVDV (evolution for high-speed integrated data and voice) are enhancements, accepted as standards in 2004. CDMA 2000 3x uses three 1.2288 Mbps channels.
UMTS	UMTS (universal mobile telecommunication system) supports both 3GPP and 3GPP2. It communicates at data rates of 100 kbps to 2 Mbps. It combines CDMA for bandwidth efficiency and GSM for compatibility. It supports several technologies for transmission and gives a framework for security and management functions. It uses DS (direct sequence) CDMA and supports a 3.84 Mbps chipping rate (Section 4.2.1). For example, the BlackBerry 7130e device has CDMA 2000 1x EVDO (evolution data optimized) support and can also be used as a wireless tethered modem. (Tethered modem means when a laptop or PC is connected to the device, the device works as wireless modem for it.)

A WPAN standard is the Bluetooth IEEE 802.15.1. It operates at a frequency of 2.4 GHz radio spectrum, which is identical to that of the IEEE 802.llb WLAN standard. Bluetooth provides short distance (1 m to 100 m range as per the radio spectrum) mobile communication. The data rates between the wireless electronic devices are up to 1 Mbps. Examples of such communications are transmissions

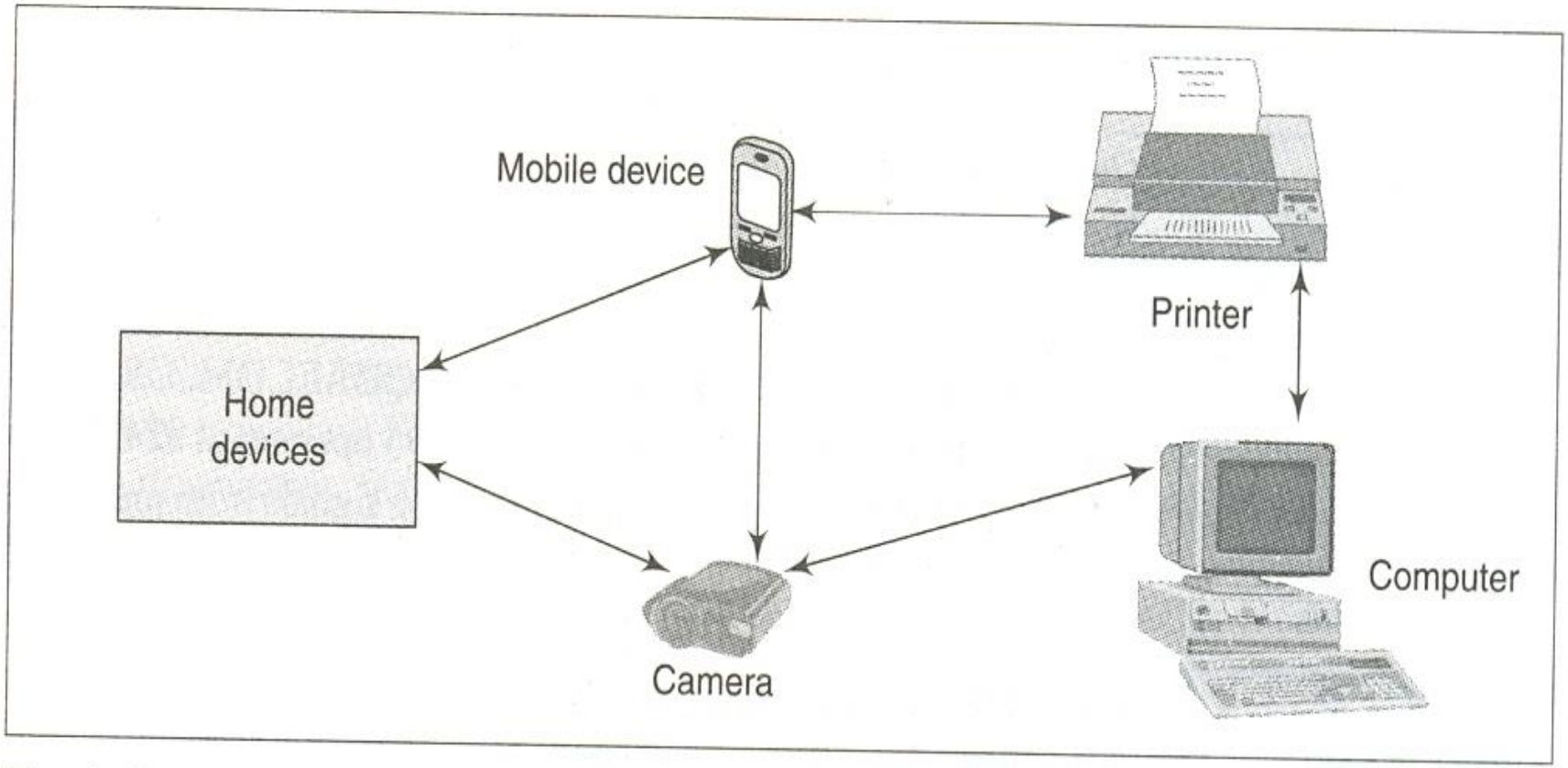


Fig. 1.10 Wireless personal area network using Bluetooth, ZigBee, or IrDA protocols

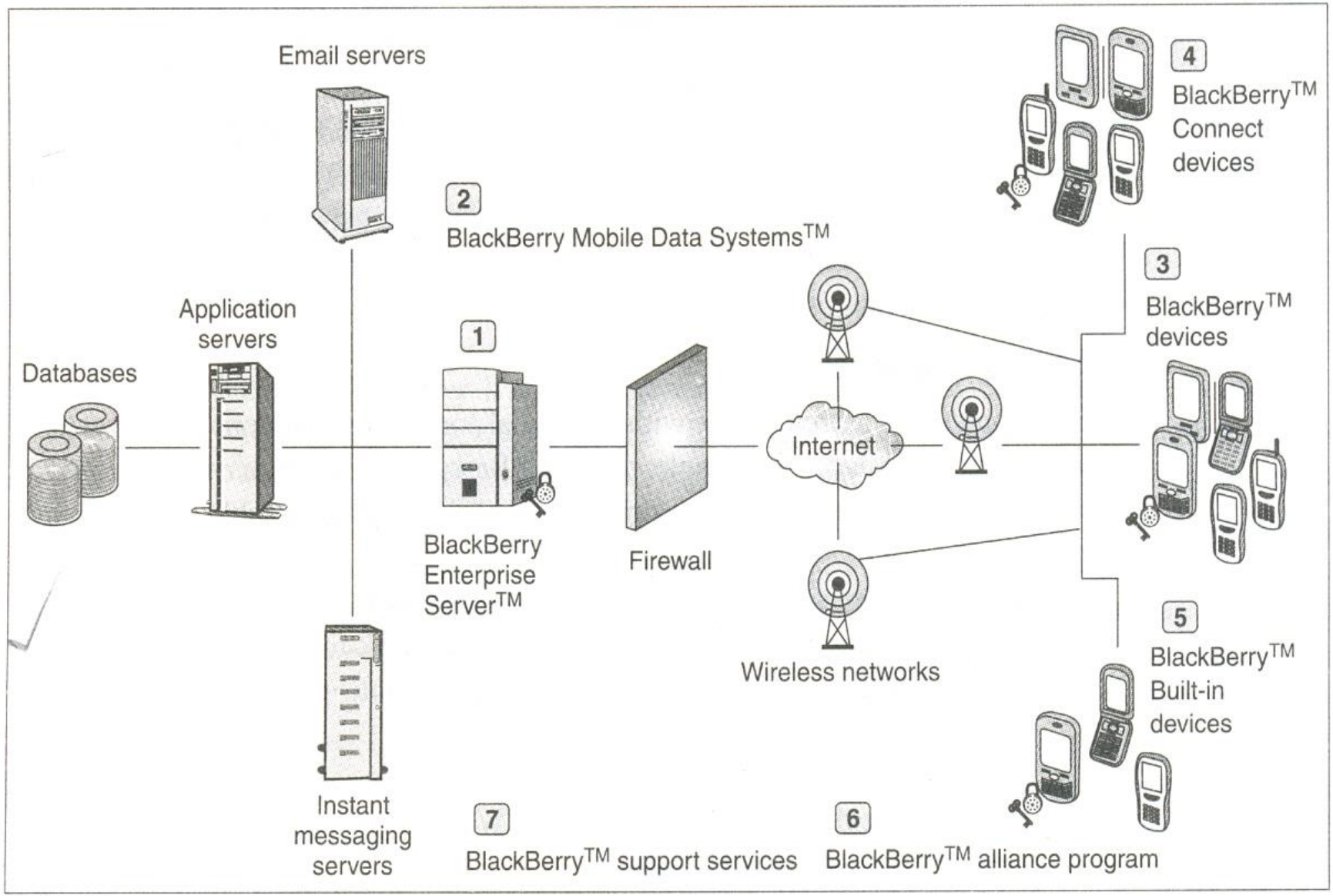


Fig. 1.12 Enterprise-solution architecture in a BlackBerry device

Mobile Commerce

- An example of m-commerce is as follows. Mobile devices are used to obtain stock quotes in real time or on demand. The stock purchaser or seller first sends an SMS for the trading request, then the stock trading service responds in the same manner, requesting authentication. The client sends, through SMS, the user 10 and password. The client is then sent a confirmation SMS to proceed further. The client sends an SMS for a specific stock trade request. The service provider executes the trade at the stock exchange terminal. The process is completed online within a minute or two.
- Another example of m-commerce is that of a purchaser relating their intention to buy a product to the mobile purchase services provider through SMS. The service provider sends the prices of that product in ascending order of the price at different stores for the same product. The customer then requests the service provider to place the order to the cheapest and nearest supplier.
- Mobile devices are also being increasingly used for e-ticketing, i.e., for booking cinema, train, flight, and bus tickets

Mobile Computing Architecture

- This section outlines the architectural requirements for programming a mobile device. It will provide an overview of programming languages used for mobile system software (Section 1.3.1). An operating system is required to run the software components onto the hardware. Section 1.3.2 gives an overview of the operating system functions. The following subsections will summarize the middleware components deployed in mobile devices and systems and layered structure arrangement of mobile computing components. Finally, this section discusses the protocols and layers used for transmission and reception of data in a network of the mobile devices and systems.

1. Programming Languages

A variety of programming languages is used in the mobile computing architecture. One popular language used for mobile computing is Java. This is because of the most important characteristic of Java, i.e., platform independence-the program codes written in Java are independent of the CPU and as used in a system. This is due to a standard compilation into byte codes.

Java 2 has a standard edition called 12SE. It has two limited memory sized editions-J2ME (Java2 Micro edition) and JavaCard (Java for smartcard). These two are the most used languages in mobile computing and for developing applications for a mobile device platform. The Java 2 enterprise edition (J2EE) is used for web and enterprise server-based applications of mobile services. Chapters 13 and 14 will describe the language features and development tools in detail.

C and *C++* are other widely used programming languages. For these languages, program compilation depends on the CPU and as used. One can use the in-line- assembly codes directly in a *C/C++* program. The advantage of *C/C++* is that it gives compact machine-specific codes. Visual *C++* and Visual Basic are also used for developing applications for a pocket PC with a Windows platform.

jkm.cse@gmail.com

2. **Operating Systems**

An operating system (OS) enables the user to run an application without considering the hardware specifications and functionalities. The as also provides as functions which are used for scheduling multiple tasks in a system. The as provides management functions (such as creation, activation, deletion, suspension, and delay) for tasks and memory. It provides the functions required for the synchronization of multiple tasks in the system. A task may have multiple threads. The as provides for synchronization and priority allocation of threads.

An as also provides interfaces for communication between software components at the application layer, middleware layers, and hardware devices. It facilitates execution of software components on diversified hardware. An as provides configurable libraries for the GUI (graphic user interface) in the device. User application's GUIs, VUI (voice user interface) components, and phone API (application programming interface) are a must in many user-operated devices.

- The as supplies these. The as also provides the device drivers for the keyboard, display, USB, and other devices.
- Sections 14.2-14.4 wi II describe some popular operating systems used in mobile computing (such as the Symbian as, the Windows CE, and the PalmOS).

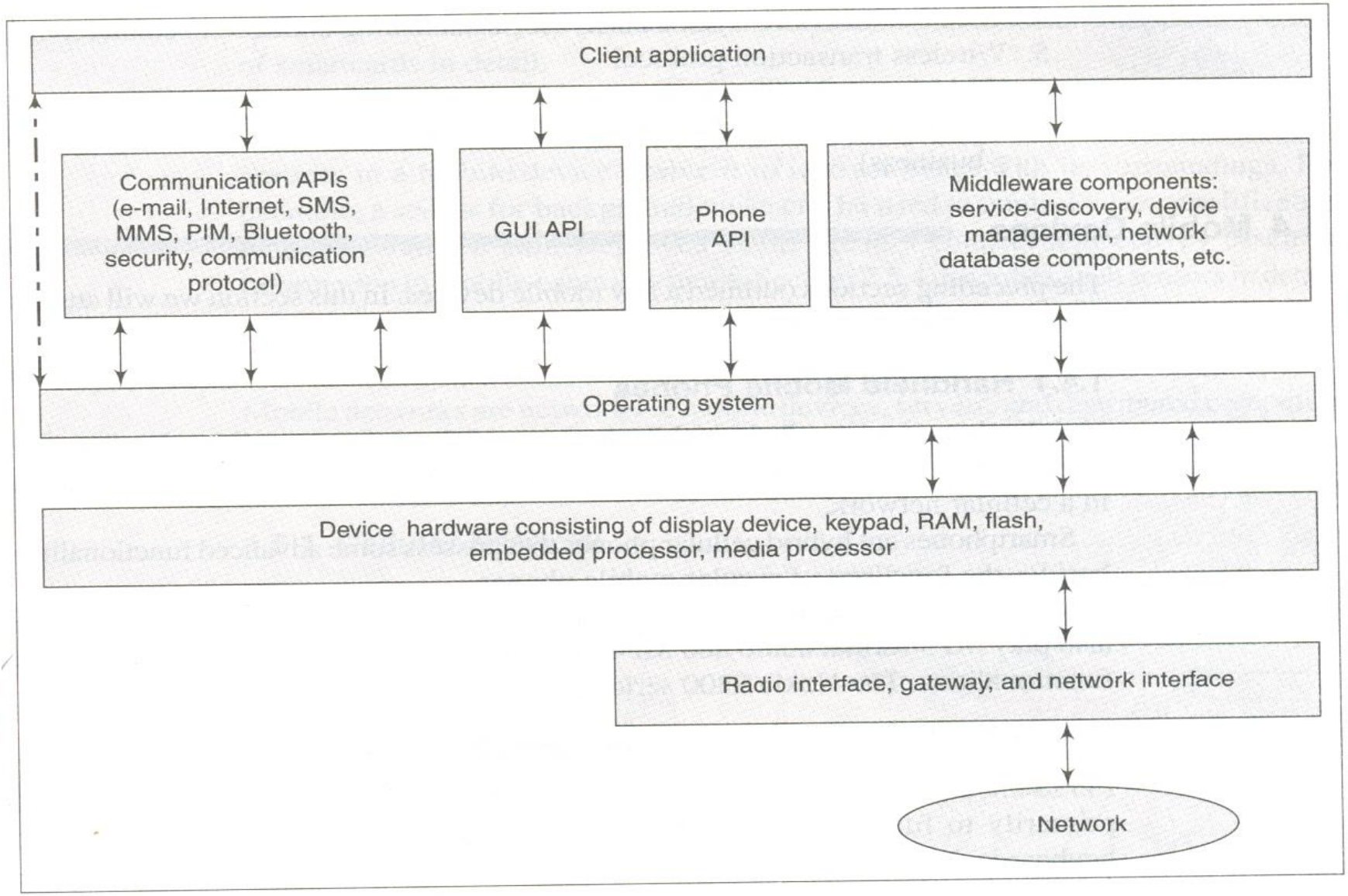


Fig. 1.13 Mobile computing architecture for a mobile device

5. Protocols

- Interchanges between two diversified and distributed components need protocols and standards. Mobile computing services use a number of mobile communication protocols (Fig. 1.9), such as GSM900, *GSM900/180011900*, UMTS, and i-Mode. Chapter 12 describes WPAN protocols (e.g., Bluetooth, IrDA, and Zigbee) and WLAN protocols (e.g., 802.11 a and 802.11 b) and the wireless application protocol (WAP) is the communication protocol for enabling web pages on a mobile device.

6. Layers

There are different layers in network transmission and reception or in interchange of information, such as the WAP protocol layers. The OSI (open standard for interchange) seven-layer format is as follows:

1. Physical for sending and receiving signals (e.g., TDMA or CDMA coding)
2. Data-link (e.g., multiplexing)
3. Networking (for linking to the destination)
4. Wireless transport layer security (for establishing end-to-end connectivity)
5. Wireless transaction protocol
6. Wireless session protocol
7. Wireless application environment (for running a web application, e.g., mobile e-business)

Mobile Devices

The preceding sections outlined a few mobile devices. In this section we will attempt at classifying such devices into a few broad categories.

1. **Handheld Mobile Phones**
2. **Handheld Personal Digital Assistants and Palmtop Computers**
3. **Smartcards**
4. **Smart Sensors**

Mobile System Networks

Mobile networks are networks of mobile devices, servers, and distributed computing systems. There are three types of mobile networks. These are described in the following sections.

1. **Cellular Network**
   Figure 1.14 shows the cellular network architecture. A cell is the coverage area of a base station, connected to other stations via wire or fibre or wirelessly through

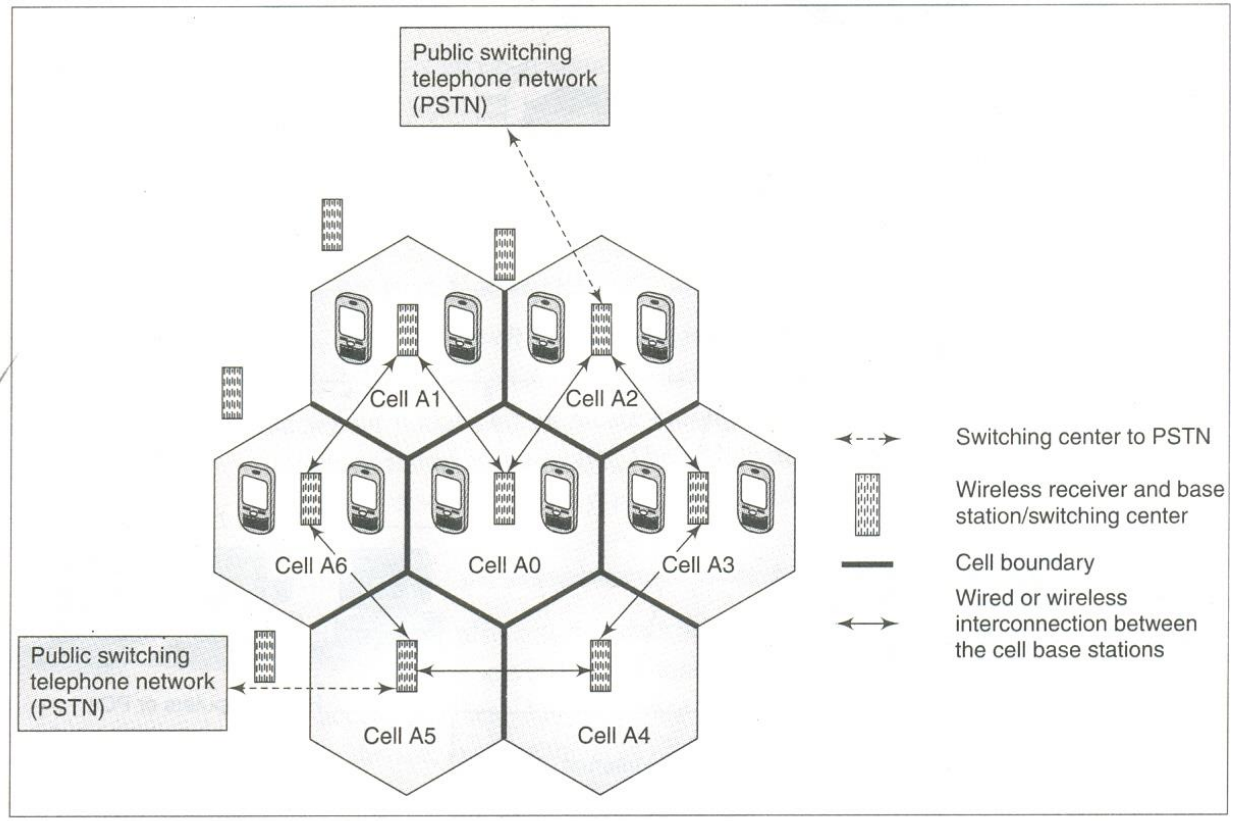


Fig. 1.14 Mobile communication using a cellular network

switching centres. The coverage area defines a cell and its boundaries. Each cell has a base station. A base station functions as an access point for the mobile service. Each mobile device connects to the base station of the cell which covers the current location of the device. All the mobile devices within the range of a given base station communicate with each other through that base station only. Section 2.1.3 will detail the functioning of a cellular network.

WLAN Network and Mobile IP

1.5.2 WLAN Network and Mobile IP

Figure 1.15 shows the WLAN network architecture. Sections 5.1 and 12.1 will discuss the details of mobile IP and WLAN networks, respectively. A mobile device, such as a pocket computer or a laptop, connects to an access point called a hotspot. The access point, in turn, connects to a host LAN which links up to the Internet through a router. Thus, connectivity is established between the Internet, two LANs, mobile devices, and computers.

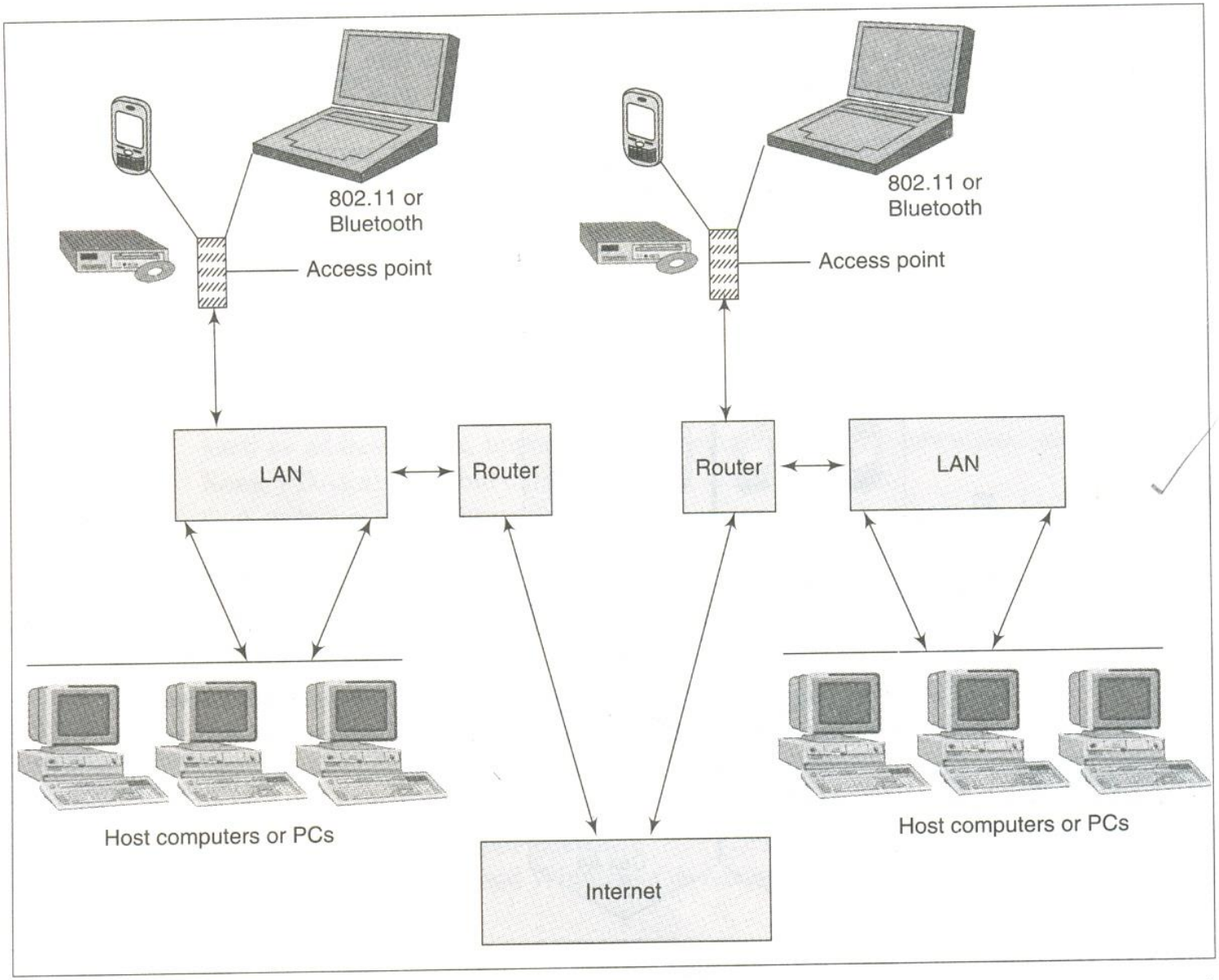


Fig. 1.15 Communication between mobile devices using a WLAN network through access points (hotspots)

Ad hoc Network

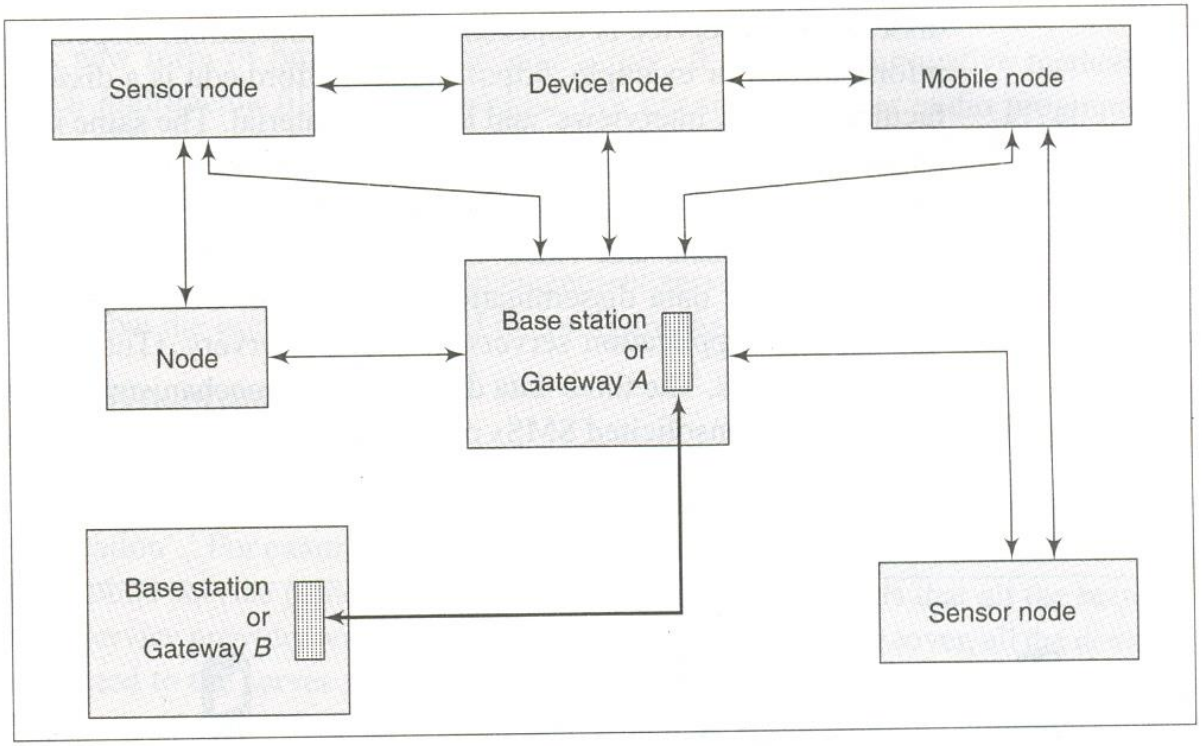


Fig. 1.16 Communication of mobile nodes and sensor nodes directly and using a base

Figure 1.16 shows ad hoc network architecture. Sections 11.2–11.4 will give the detailed features of ad hoc networks. The figure shows that the nodes, mobile nodes, and sensor nodes communicate among themselves using a base station. The base stations function as gateways. The ad hoc networks are deployed for routing, target detection, service discovery, and other needs in a mobile environment.

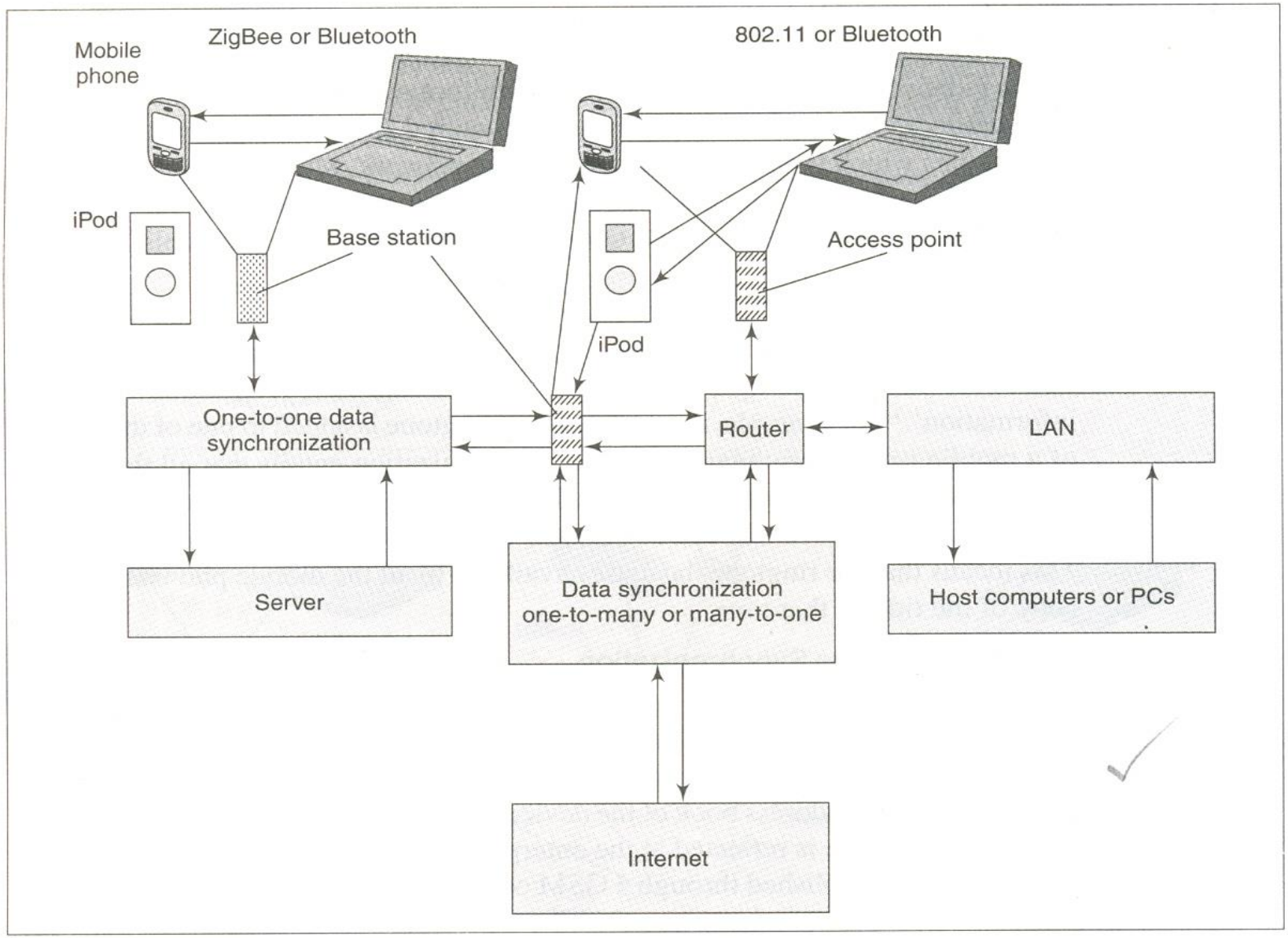


Fig. 1.18 Data synchronization paths in a mobile network

Security

- Security is important for maintaining privacy and for mobile e-business transactions. Wireless security mechanisms must provide security of the data transmitted from one end point to another. It must provide for wire-equivalent privacy and non- repudiation when some data is sent to an end point. There must be no denial of service to authenticated object(s).
- A serving station must be authenticated before it can provide service to mobile devices. Figure 1.20 shows the authentication method of security in case of GSM. The location registry at the home base-station sends a 128-bit random number, *n* 128. The mobile device calculates the response, *r32*, using *n128*. Then the secrecy code, S, at the SIM (subscriber identity module) and the *r32* are used to calculate *RS32*. The station receives the *RS32* and compares it with the calculated (from S and *n128)* signed number *RS32'*. If they are equal, the mobile device present in that cell stands authenticated. Both, the mobile device and the station, use 64-bit encryption when transmitting the *RS32* and *n128*, respectively. Only messages for authentication are encrypted in GSM. Section 3.7 will give the details.
- The WLAN security standard is IEEE 802.1Ib. It provides WEP (Wired equivalent privacy). The 802.11i caters to enhanced security needs. There is WAP security at the transport layer (Section 12.2.3).

Cryptography Algorithms

- The purpose of cryptography is to keep private information from getting into the hands of unauthorized agents. Encryption is the transformation of data into coded formats. Encrypted data can be decrypted (transformed back to an intelligible form) at its destination.

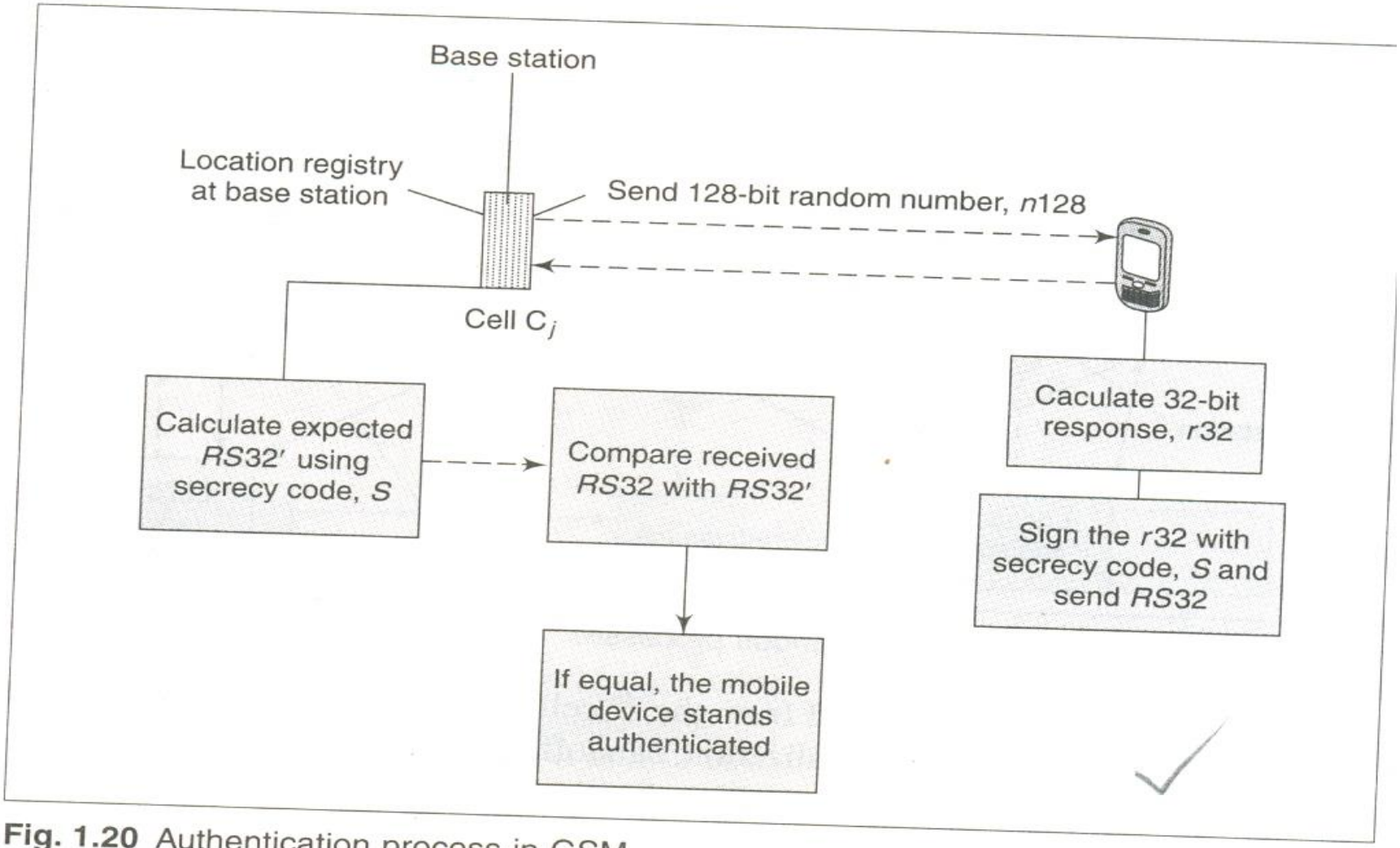


Fig. 1.20 Authentication process in GSM

- Various cryptography algorithms are used for encryption and decryption of transmitted data. These algorithms enable the receiver and the sender to authenticate data as well as discover if data security has been compromised during transmission. Cryptography algorithms generally use a secret key to encrypt data into secret codes for transmission. For example, the RSA (Rivest, Shamir, Adleman) algorithm is a cryptography algorithm used for private key generation. Cryptography algorithms can be classified into two categories-symmetric and asymmetric (Section 10.2).
- Cryptographic algorithms are used to create a *hash* of the message or an *MAC* (message authentication code). A hash function is used to create a small digital fingerprint of the data to be transmitted. This fingerprint is called the hash value, hash sum, or simply, hash. The hash of the message is a set of bits obtained after applying the hash algorithm (or function). This set of bits is altered in case the data is modified during transmission. Message authentication codes (MAC) are also used to authenticate messages during transmission. The MAC of a message is created using a cryptographic MAC function which is similar to the hash function but has different security requirements. The receiver reviews the hash or the MAC of the received message and returns it to the sender. This exchange enables the sender and the receiver to find out if the message has been tampered with and thus helps verify message integrity and authenticity. Table 1.5 provides various security standards.

MOBILE (IN)SECURITY: WHO'S LISTENING?

Smart Phone Growth

- The day when everyone has a PC in their pocket has arrived –
- Annual growth rate is 150%
- Three things driving growth –
  - Increasing amount of time we spend online whether business or pleasure
  - Instant gratification-hard to wait to check messages or update status
  - Lifestyle patterns, social networking

National Science Foundation <nsf.gov> 5/21/2009

All Gs Considered

- 1G Phones – Analog telephones with no texting or messaging capabilities
- 2G Phones – Digital telephones with personal communications services (PCS), like paging, caller ID and e-mail
- 3G Phones – Multimedia smart phones feature increased bandwidth and transfer rates to accommodate Web-based applications and phone-based audio and video files
- 4G Phones not widely available now
  - Feature real-time transfer rates

Aren't Smart Phones Secure?

1. Proliferation of mobile devices with powerful computing resources
2. No massive malware outbreak to date = *no panic about security*
   - iPhone SMS attack in July 2009 changed that perception to some degree
3. We trust smart phones & think they are safe
   - We have the mistaken sense they are immune to security threats
4. Smart phones typically lack security features, like antivirus, found on other computers

Will It Happen in 2020?

What Keeps Malware off Mobiles

1. Code signing programs
   a. Mobile network operators, OS vendors and handset manufacturers all have code signing programs to control what code is run on the phone
   b. Changing with Android & jail breaking
2. Fragmented market
   a. Nothing like the market share Microsoft Windows has on computer
   b. Malware authors choose minority platform

Developers' Responsibility

- Mobile application developers must learn how best to manage mobile application security risks
  - Limited memory and CPU
  - Multiple security models
  - *Always on* network
- Knowing the risks and how to respond to them is the only hope for creating secure software

Smart Phones Difficult to Protect

- Easily stolen: theft is single largest problem
  - You put it down for a minute & walk away…
  - Falls out of your pocket somewhere
  - Mobility = higher risk
- Protection options not well known
  - Encryption options are all different
- Eavesdropping options are available
- More types of smart phones = complications
  - No standardization at this time , which is both good and bad

Smart Phones ‘R Pocket Computers

- Most commonly used phones, as defined by operating system (OS) –
  - Android (Android OS)
  - BlackBerry (RIM OS)
  - iPhones / iPod touch (iPhone OS)
  - PalmPre (WebOS)
  - Windows Mobile (WinMobile OS)

Basic Protection All Smart Phones

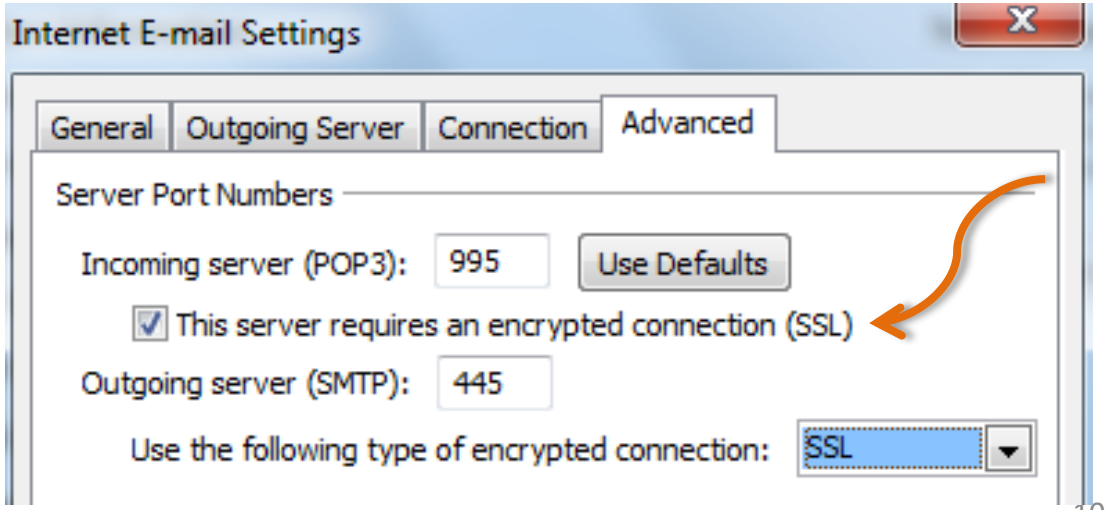
- Passcode
  - Enable at least 4 digits but this also depends upon IT policies
  - Exceeding the number of allowed password attempts deletes all data
- Auto-Lock
  - Locks the screen after a pre-set time period of non-use (consider 30 minutes or less)
  - Passcode-lock enhances auto-lock
  - By itself not exactly a security feature but combined with passcode protection, it's essential security

Secure a BlackBerry (BES)

- If you connect to the BlackBerry Enterprise Server (BES) at UVa or on a corporate intranet, ask the BlackBerry server admin to enforce the following options – and ***test*** them
  - Passcode protection
  - Remote Delete
  - Encryption (Content Protection)
- Use the Auto-Lock feature, which together with passcode protection is essential security

Secure a BlackBerry (BIS)

- If you connect to the BlackBerry Internet Service (BIS), enable passcode and auto-lock features
- Use *POP3s* over SSL to increase security from the BIS server back to your mail server.
  - The data is secure from your device back to the BIS servers, because it uses SSL over a secure network

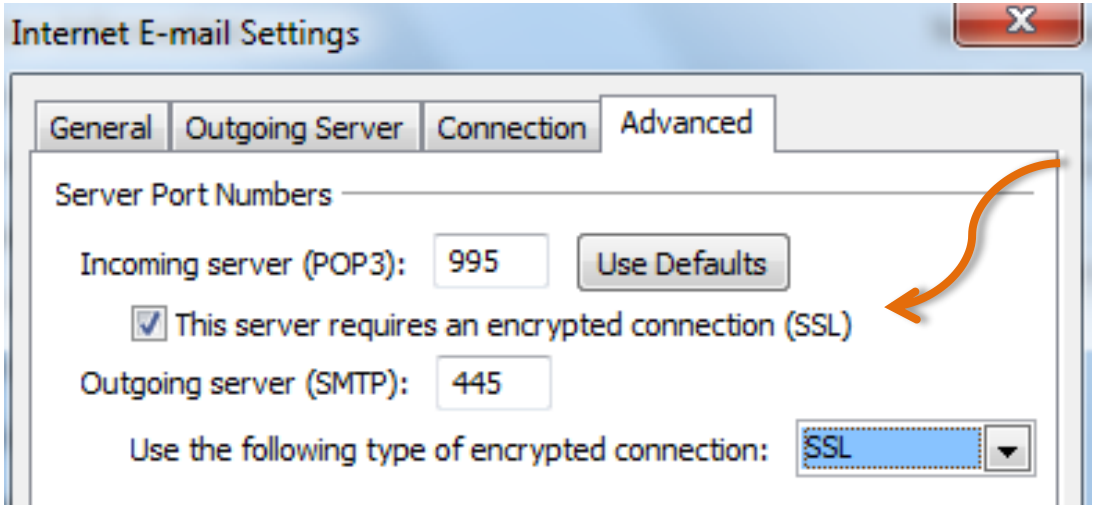


Secure Windows Mobile SP

- If you connect to a Windows Exchange Server at UVa, or on a corporate intranet, ask the IT folks to enforce the following options, and
  test them
  - Passcode protection
  - Remote Delete through Outlook Web Access
  - Encryption* may only be possible if you use a removable flash storage card, even if you connect to an Exchange server
  - Use the Auto-Lock feature, which together with passcode protection is essential security

Secure WinMobile Non-Business

- If you are a non-business user, encrypt* with removable flash memory storage card
- Antivirus protection from third-parties
- Remote delete if GPS feature installed
- Use POP3s over SSL, if possible, to increase security to your mail server



Secure an iPhone

- If you connect to the Windows Exchange Server at UVa, or on a corporate intranet,
  ask the IT folks to enforce the following options, and *test* them
  - Passcode Lock requires you enter a four-digit code to use the iPhone again
  - Remote Delete through Outlook Web Access
  - Enable the iPhone “Ask to Join Networks” function

Center for Internet Security (CIS) released free guidelines to help organizations develop custom policies related to iPhone use

Secure an iPhone Part II

- *Auto-Lock* locks the touch screen for a preset time period after not being used for one, two, three, four or five minutes. Turned on by default but can be disabled altogether
- *Password-protect* the SIM card on a 3G
- The *Erase Data* function lets you completely wipe your iPhone after 10 failed passcode attempts

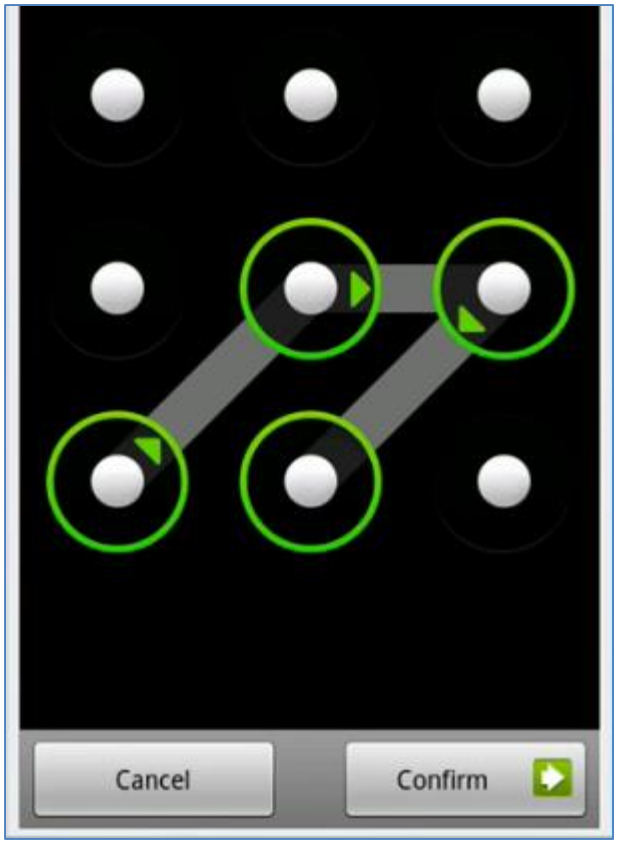
Secure an iPhone Part III

- Turn off Text Messaging Preview
- Turn off Safari Auto-fill
- Use POP3s over SSL to increase security
  - 3G iPhones use SSL by default over POP, IMAP and SMTP
- Device restrictions are available if your children use an iPhone, iPod or iPod touch connecting to iTunes (explicit songs, etc.)

Secure a Palm Pre (WebOS)

- Original PalmOS does not allow for encryption or timed auto-lock
- New Palm webOS enables these features
- Both operating systems can connect to an Exchange server through ActiveSync
  - Remote Delete is available through Outlook Web Access
  - Encryption may only be possible if you use a removable flash storage card and a third-party provider
- Non-business users –
  - Use POP3s over SSL to increase security

Android's Auto-Lock Feature



Viruses and Smart Phones

- How smart phone viruses spread –
  - Internet downloads (file-sharing, ringtones, games, phony security updates, etc)
  - Bluetooth virus (short range)
  - Multimedia Messaging System (MMS) virus spreads using the device address book
- Viral epidemics – a highly fragmented smart phone market share has inhibited outbreaks
- Only smart phones susceptible to viruses
  - Phones that can only make and receive calls are not at risk

Internet, Bluetooth, and MMAs

- In all of these transfer methods, the user has to agree at least once (and usually twice) to run the infected file
- But smart phone virus writers get you to open and install their product the same way computer virus writers do:
  - The virus is typically disguised as a game, security patch or other desirable application

Bluetooth Threat Vectors

- Bluejacking - sending unsolicited messages over Bluetooth (BT) to BT-enabled devices
  - Limited range, usually around 33 ft on mobile phones
- Bluesnarfing - unauthorized access of information from a wireless device through a BT connection
  - Allows access to a calendar, contact list, emails and text messages, and on some phones users can copy pictures and private videos
  - Possible on any BT-enabled device
  - Either can do serious harm - Bluesnarfing copies info from victim's device and is more dangerous

Lock Down Bluetooth!

- Bluetooth is default-on
  - Wastes your battery
  - Leaves you open to Bluetooth-based attacks – most common at this time

Social Engineering Threats

- The best security in the world will *not* help you if –
  - You click on an phishing email and give your personal information
  - You click on a SMS/text message that appears to come from your carrier
  - You respond to a vishing phone call*
- Never give information via email or by phone or on the web, unless you initiate the exchange

http://ourmidland.com/articles/2010/02/08/police_and_courts/2412111.txt

Smart Phone Spyware is Real

- Configure default application permissions to be more restrictive
- Don't just download any and all games, applications, security software you come across, or messages from your carrier
- Avoid granting applications “trusted application” status, which grants untrusted applications additional privileges

- Beware ÜberTwitter, which demands full access to your BlackBerry

http://www.sfgate.com February 8, 2010

Twitter on Smart Phones

- Two Security Issues
  - Link shorteners like TinyURL lead users to unknown destinations
  - Single login system
- Phishers use Twitter in attack May 2009
  - Bogus accounts of “hot” women
  - Tiny URLs obfuscated real sites

Eavesdropping

- Last year Karsten Nohl, a UVa PhD graduate, cracked the secret code used on 80% of the world's phones
- Mobile interception, as a result, is now within the reach of "any reasonable well-funded criminal organization"
- You and I cannot fix this problem, but it's not likely to affect us individually

http://www.nytimes.com/2009/12/29/technology/29hack.html

Different Kind of Eavesdropping

- Anyone can install eavesdropping software on your smart phone, as long as they have access to your phone even for a few minutes
- Subtle signs that could suggest someone is secretly tapping your cell phone –
  - Cell phone battery is warm even when your phone has not been used
  - Cell phone lights up at unexpected times, including occasions when phone is not in use
  - Unexpected beep or click during phone conversation
- Passcode and Auto-lock to protect your phone
  - Don't share the passcode with anyone, even spouse

http://www.wthr.com – Tapping Your Cell Phone 6-29-2009

Jealous Husband Scenario

- 5 minute physical access to an iPhone, an Apple $99 developer license, a USB cable
- Install SpyPhone, and send the report
- Delete the report from sent emails,
  - Delete SpyPhone

Paris Hilton's Phone

- Remember when someone got his hands on Paris Hilton's contact list?
- Not the result of a virus, and nobody hacked into Hilton's phone
- Mobile phone servers hold on to certain types of information, such as contact lists (in case the user's phone locks up) and recent calls (for billing purposes)
- The enterprising hacker got into T-mobile's servers and stole the information from there

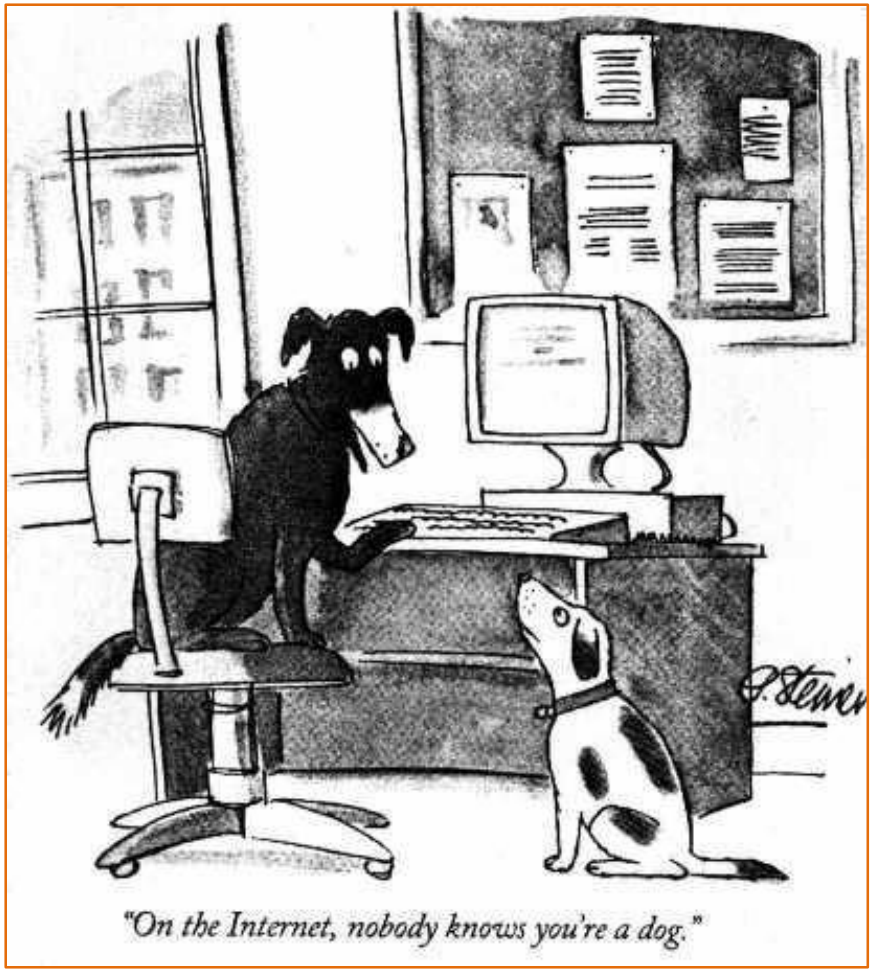
Celebrity Bling Ring

Another Potential Threat

- Researchers spoofed messages that appear to come from 611, the number carriers use to send out alerts, update notifications and other messages
  - Offered a $20 credit to collect info to stage a more targeted attack, or try to trick a user into installing malware, etc.

http://www.wired.com/threatlevel/2009/07/sms/

On the Internet, Nobody Knows You're a Dog



Any message, whether on a smart phone, computer, USB, or Facebook, on your windshield, or in your physical mailbox, can be spoofed. Verify independently.

Threats to Smart Phones 2020

- Attackers will exploit our social conditioning entering Personally Identifiable Information (PI/PII), while interacting with phone voice response to commit vishing and identity theft.[1]
- We demand more and better availability from phone service than we would from an ISP, "so the threat of a DoS attack might compel carriers to pay out on a blackmail scam."[1]
- "At this point, *mobile device capability is far ahead of security*… We'll start to see the botnet problem infiltrate the mobile world in 2010."[2]

[1]Tom Cross - X-Force Researcher, IBM Internet Security Systems
[2]Patrick Traynor - Assistant Professor, School of Computer Science at Georgia Tech
Georgia Tech Information Security Center <gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>

Layered Security – Easy Steps

- Enable passcode and auto-lock features
- Know how to remote delete quickly
- Don’t let your smart phone out of your sight or share it with friends or children
- Don’t store sensitive data (UVa policy)
- Verify independently before you click on any unknown text or email message, game, application, or “security” update

Defense-in-Depth

- Get latest firmware and software your mobile device manufacturer provides
- Maintain situational awareness when carrying any electronic device
- Watch your mobile device as you go through airport security
  - Known bad location for device theft
- Do not use insecure wireless hotspots
  - Save important transmissions until you can connect to a secure environment

GSM

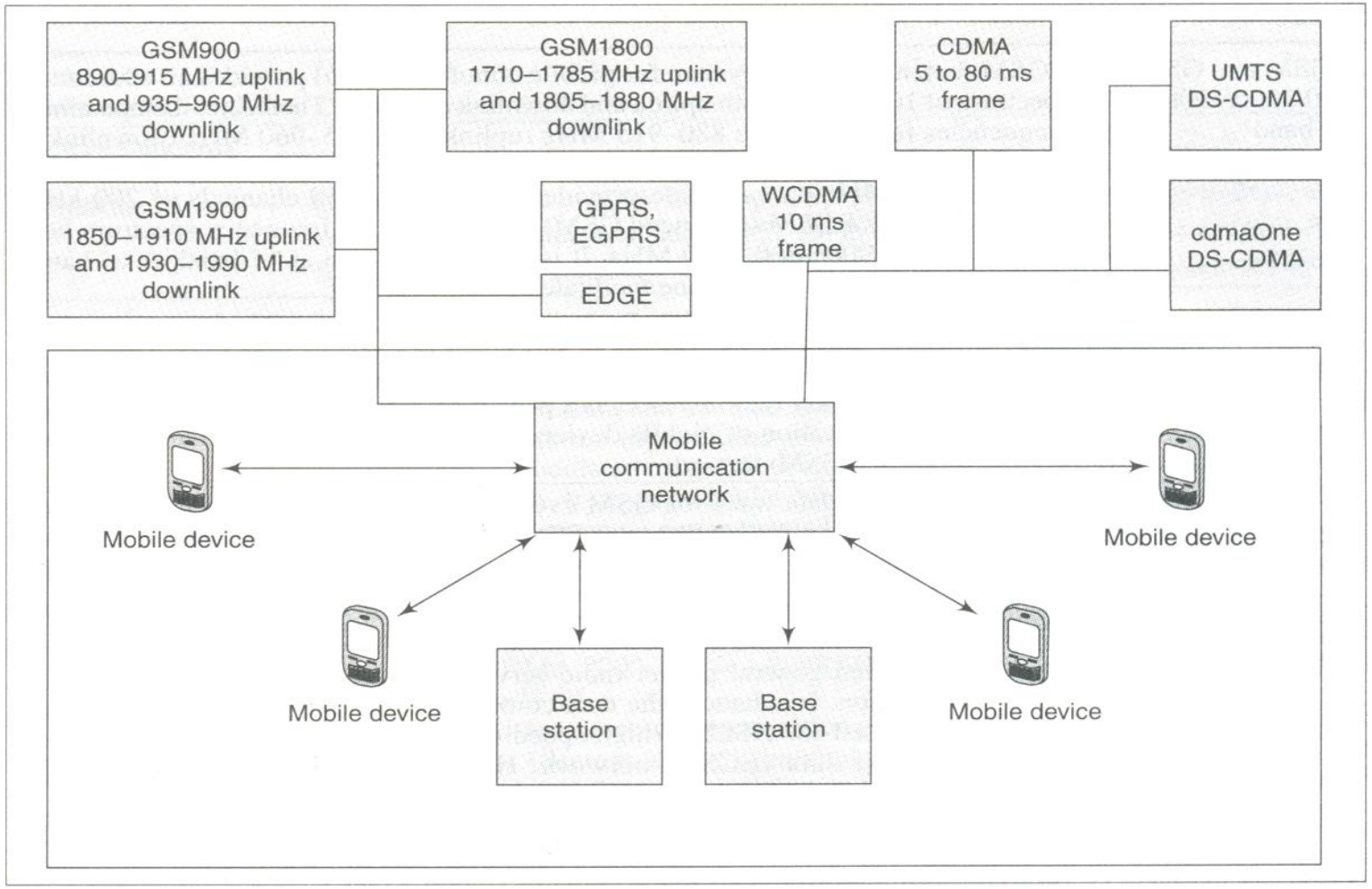


Fig. 1.9 GSM- and CDMA-based standards and a mobile communication network for long distance communication

1.2.1.2 Enterprise Solutions

Enterprises or large business networks have huge database and documentation requirements. The term 'enterprise solutions' therefore refers to business solutions for corporations or enterprises. This may include specialized hardware or software programming to help an enterprise in finding solutions for various needs such as management of storage, security, revision, control, retrieval, distribution, preservation and destruction of documents and content, etc. These days mobile devices are being increasingly used to provide enterprise solutions. The Nokia 9300 (Section 2.4.3) and the BlackBerry 7130e are examples of mobile devices designed for use in enterprises.

Figure 1.12 shows enterprise-solution architecture using BlackBerry devices. It gives access to enterprise employees and connects to an enterprise server. It provides

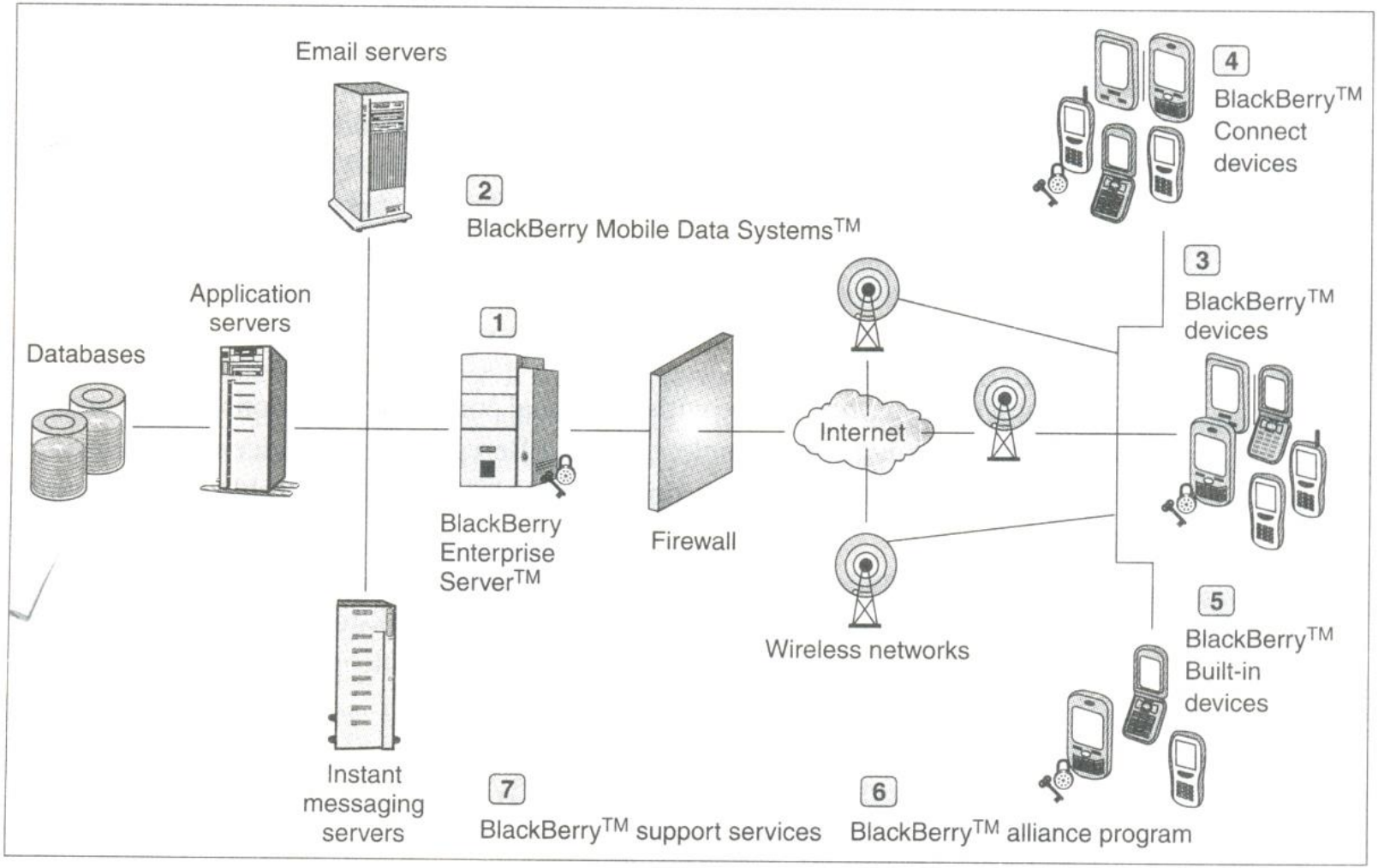


Fig. 1.12 Enterprise-solution architecture in a BlackBerry device

SYNCHRONIZATION

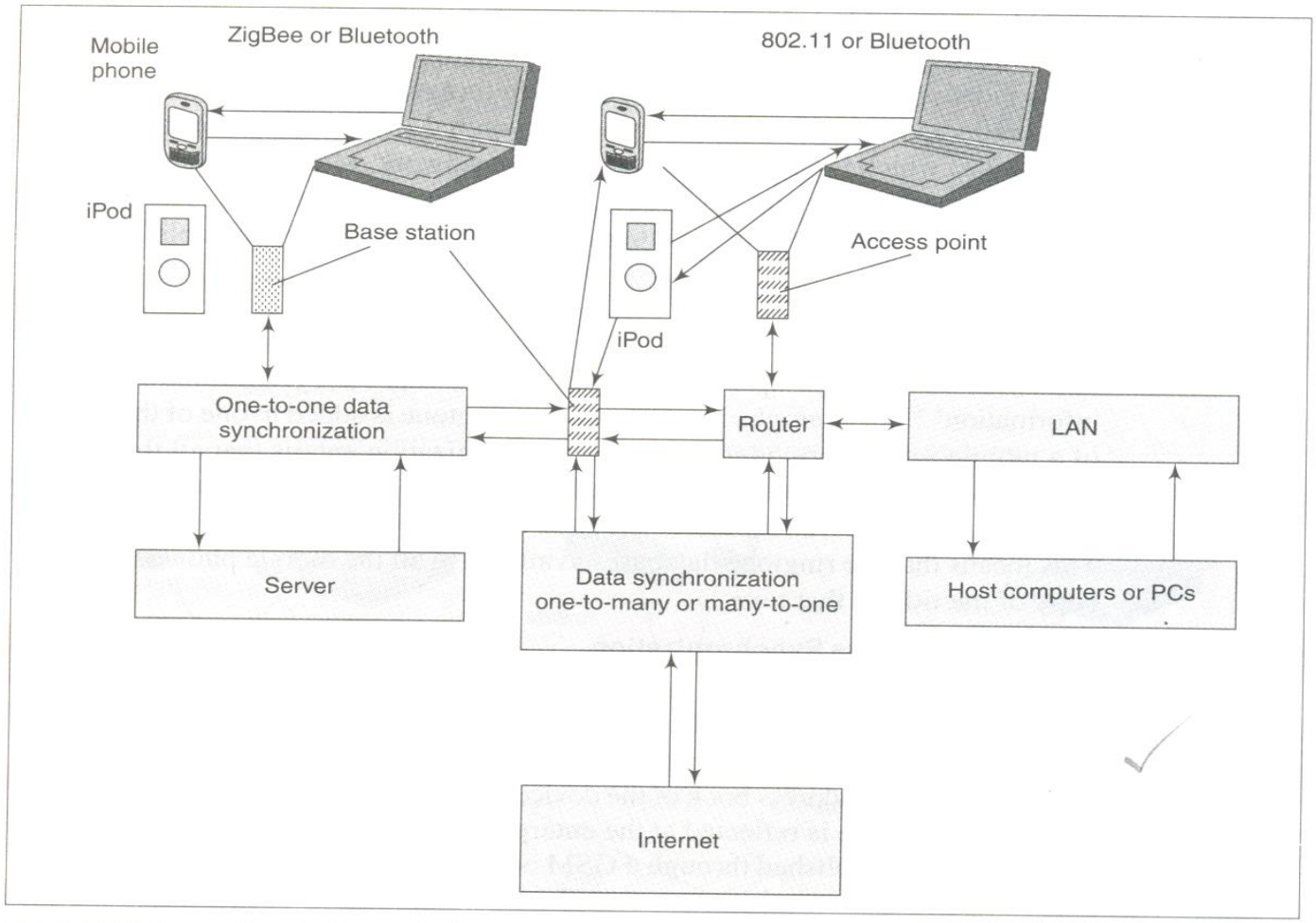


Fig. 1.18 Data synchronization paths in a mobile network

MOBILITY MANAGEMENT

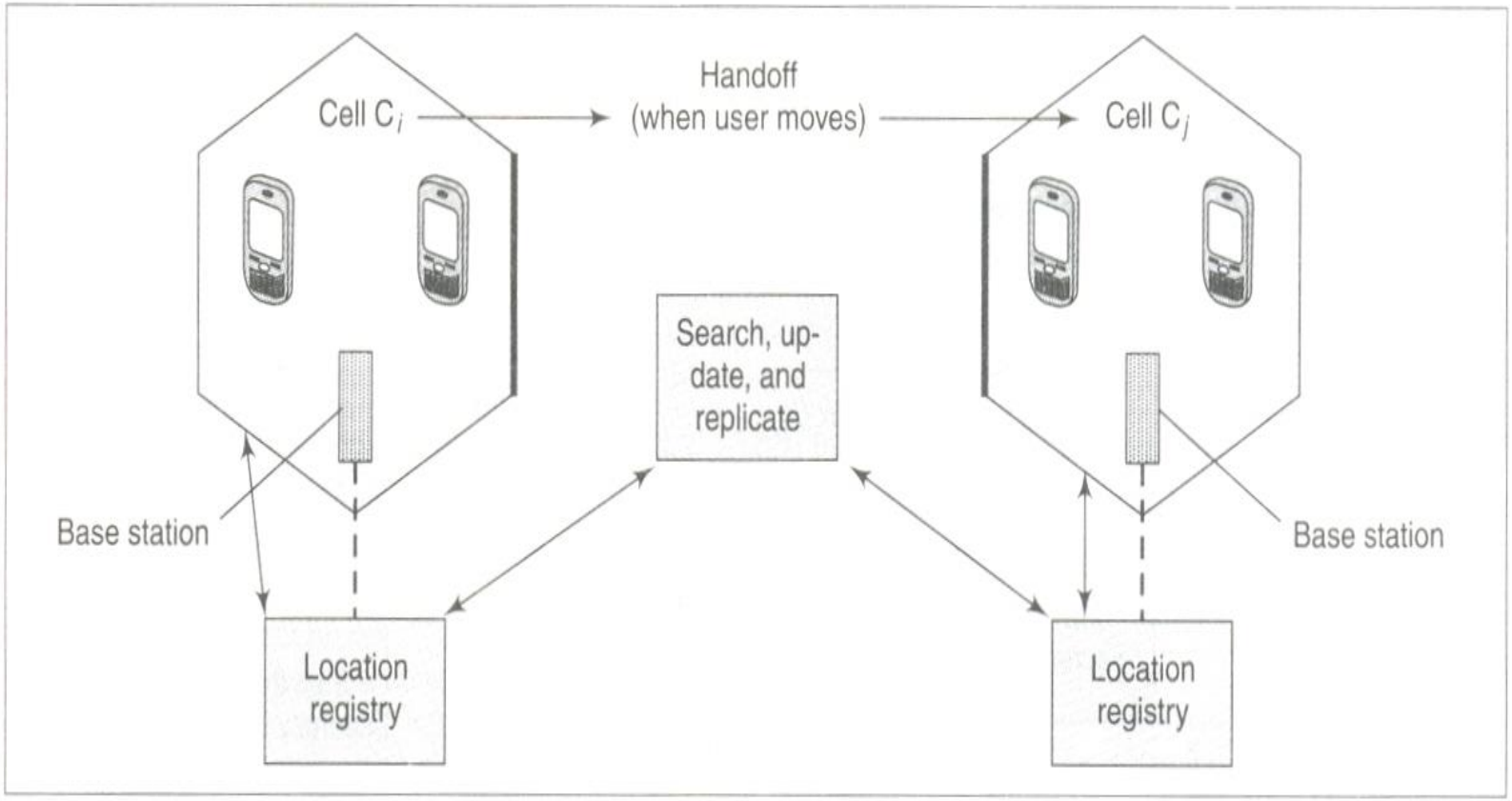


Fig. 1.19 Location registration and handoff processes

SECURITY

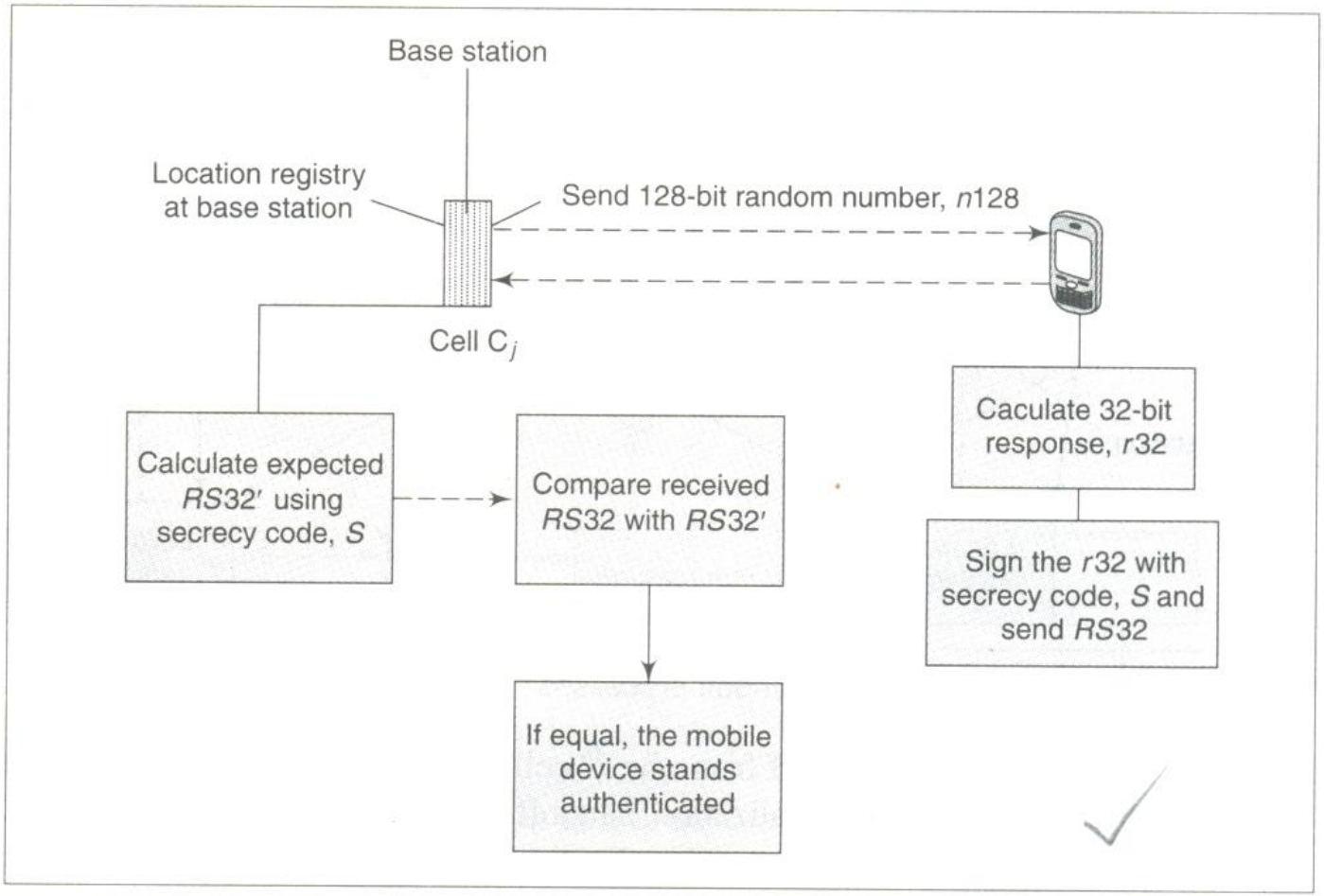


Fig. 1.20 Authentication process in GSM

GSM SYSTEM ARCHITECTURE

3.1.2 GSM System Architecture

Figures 1.9, 1.14, and 3.1 show mobile communication using base stations in cellular networks and how a mobile station, MS, communicates with a GSM public land mobile network (PLMN) which, in turn, may connect to a PSTN network. The PSTN connects to a source–destination network which acts as an interface for the destination terminal, TE. This basic outline of a GSM network, however, does not provide a detailed picture of the GSM network architecture. Figure 3.2 shows the GSM network architecture.

The network is divided into three subsystems namely, radio subsystem (RSS), network subsystem (NSS), and operation subsystem (OSS). The RSS consists of a number of base station controllers (BSC) and each BSC connects to a number of base transceiver stations (BTS) which, in turn, provide radio interfaces for mobile devices. The NSS consists of a number of mobile services switching centres (MSC). Each MSC of the NSS interfaces to a number of BSCs in the RSS. There are also home location registers (HLR) and visitor location registers (VLR). The OSS consists

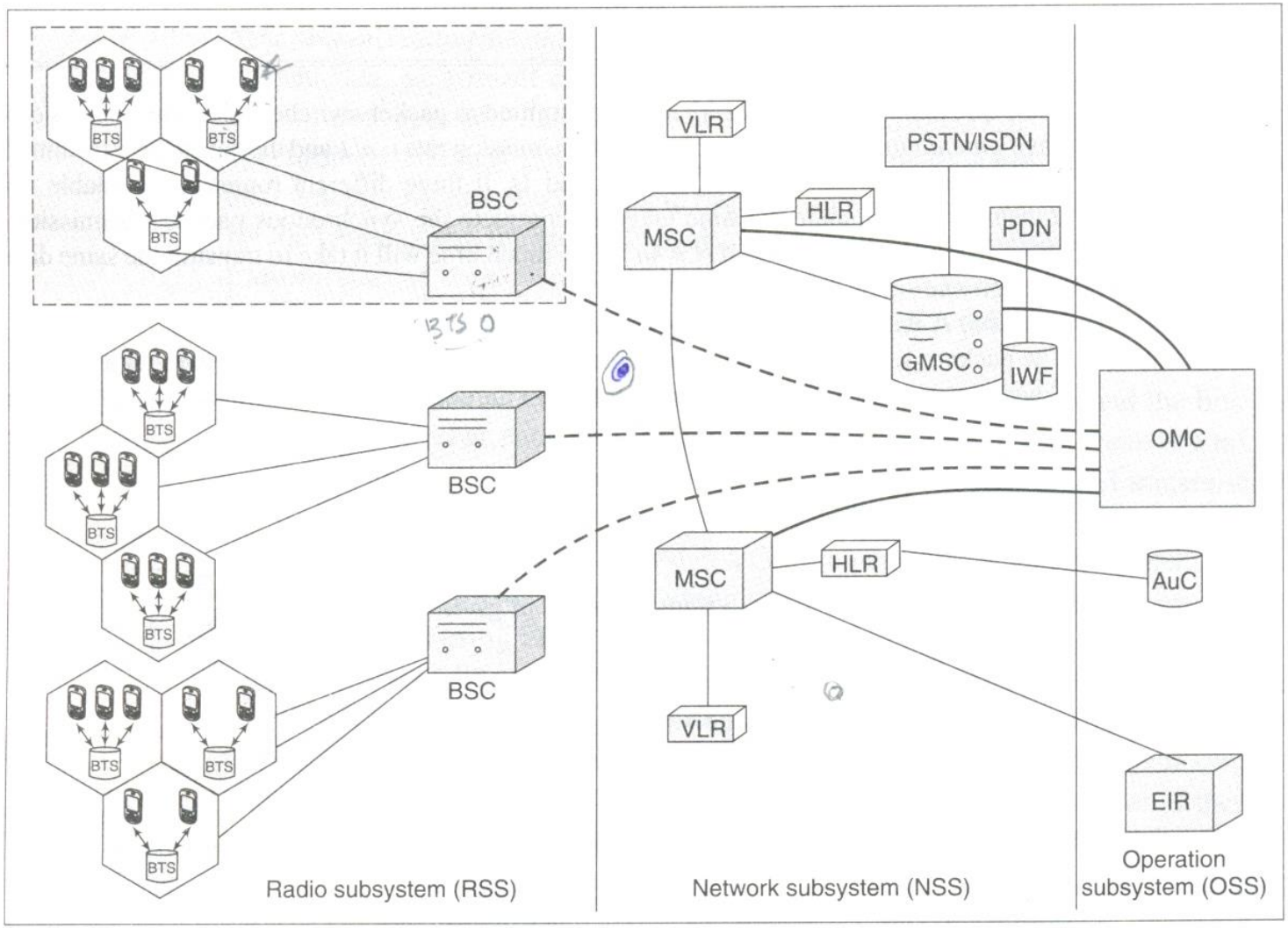


Fig. 3.2 GSM network architecture

MOBILE STATION

Mobile Station A mobile station (MS) is the mobile device or phone which connects to the GSM network. It consists of a mobile terminal (MT), which is the device (or the phone itself) with hardware and software to transmit and receive GSM data, and a user terminal (TE) through which the user receives and sends the data (this is the radio transmission system used in GSM network

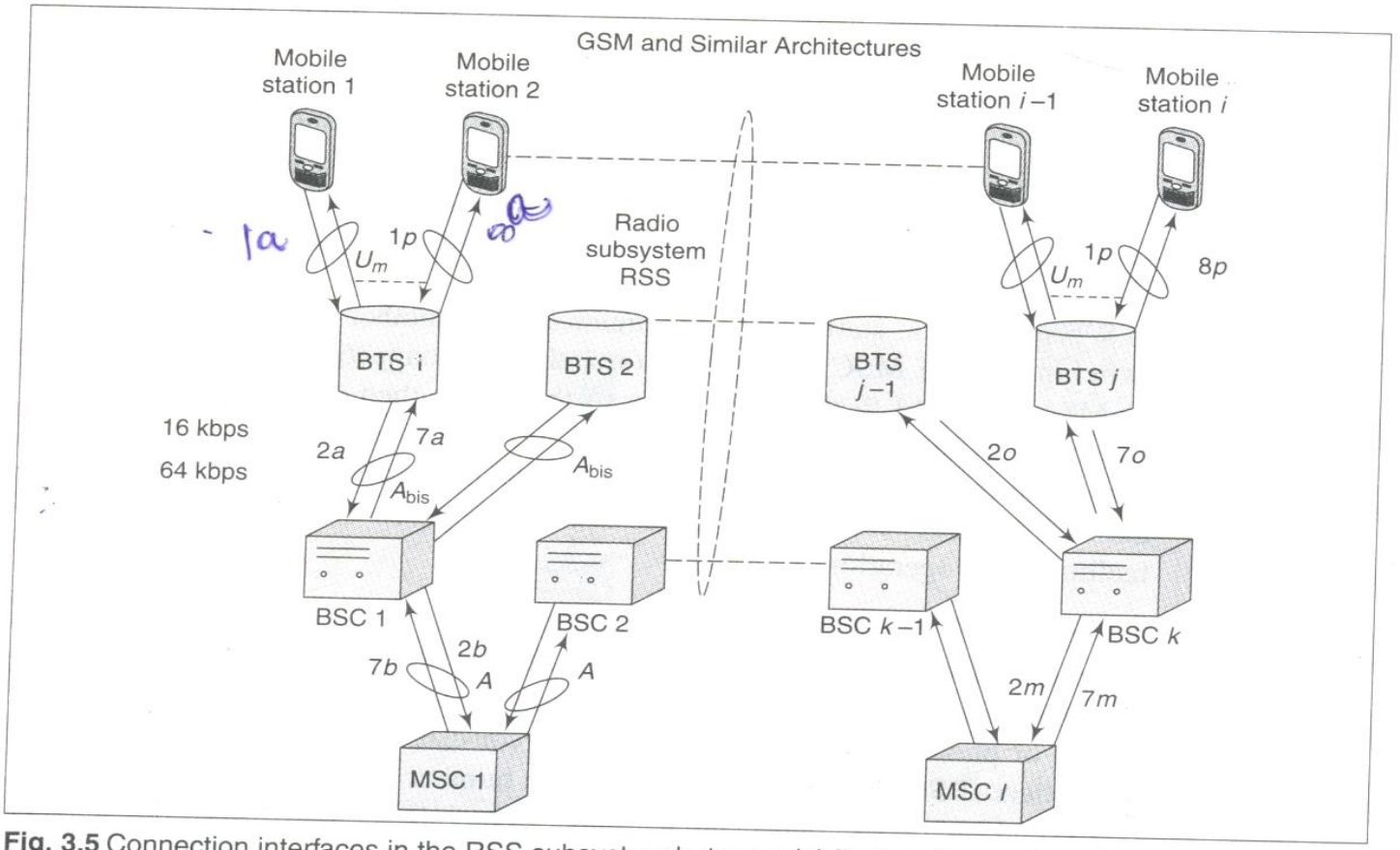


Fig. 3.5 Connection interfaces in the RSS subsystem between (a) BTS and a number of MSs, (b) BSC and a number of BTSs, and (c) MSC (in the NSS layer) to a number of BSCs ($i > j > k > l$)

mobile phones). The MT transmits through the interface U_m (Fig. 3.6) at a power of 1–2 W. Each MS has a subscriber identity module (SIM). SIM is a card inserted into the MS. It is provided by the GSM service provider. The SIM uniquely identifies the user to the service and enables the MS to connect to the GSM network. Some important functions of the SIM are as follows:

- When the MS connects to the GSM subsystems, the SIM stores a temporary mobile (dynamic) cipher key for encryption, temporary mobile subscriber identity (TMSI), and location area identification (LAI).

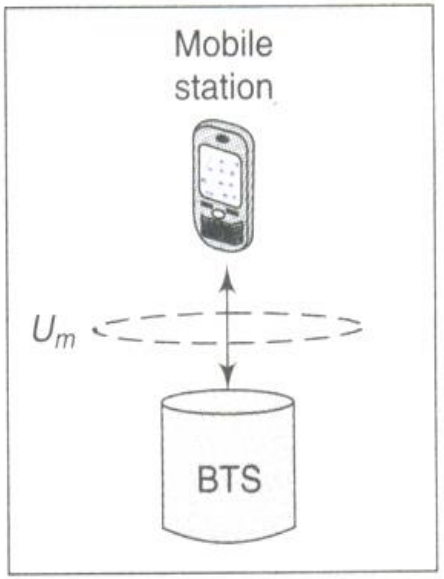


Fig. 3.6 Mobile station to BTS interface in a GSM cell

- SIM contains the following information which does not change when the MS moves into another location—(i) international mobile subscriber identity (IMSI), (ii) card serial number and type.

- The SIM contains a PIN (personal identification number). Using the PIN, the MS is unlocked when it seeks connection to another MS. The user can use the PIN to lock or unlock the MS.

- It stores the PUK (PIN unblocking key) which enables the subscriber to unlock the SIM if it is accidentally locked due to some reason.

- It stores a 128-bit authentication key provided by the service provider. The MS is authenticated by a switching centre through an algorithm using this key and a 128-bit random number dynamically sent by authentication centre. If the MS is not authenticated, the service to that number is blocked.

- The SIM also stores the international mobile subscriber identity (IMSI). The IMSI is a unique 15 digit number allocated to each mobile user. The IMSI has three parts—a three digit mobile country code (MCC), a mobile network code (MNC) consisting of two digits, and the mobile subscriber identity number (MSIN) with up to 10 digits. Mobile service providers all over the globe use an identical coding scheme for the IMSI. IMSI helps service providers in identifying and locating an MS. It helps the MS in obtaining the cipher key, TMSI, and LAI from the mobile service provider during connection setup. A TMSI is used to identify an MS during a connection for protecting the user ID from hackers or eavesdroppers (Section 3.7).

OPERATION SUBSYSTEM

3.1.2.3 Operation Subsystem

The operation subsystem (OSS) administers the operation and maintenance of the entire network. Figure 3.9 shows the OSS architecture and the interfaces to the NSS and the RSS. The main components of the OSS are the authentication centre (AuC), the operation and maintenance centre (OMC), and the equipment identity register (EIR). Each AuC is associated with an HLR in the NSS and each EIR connects to an MSC. An OMC at OSS can connect to an MSC or a GMSC in the NSS and to a BSC at RSS.

Operation and Maintenance Centre The operation and maintenance centre (OMC) monitors and controls all other network entities through the *O* interface. The OMC's typical tasks include management of status reports, traffic monitoring, subscriber security management, and accounting and billing.

Authentication Centre The authentication centre (AuC) is used by the HLR to authenticate a user. The AuC may also be a secured partitioned part of the HLR

itself. Since mobile networks are quite vulnerable to attacks, the GSM standard specifies that the algorithms for key generation should be separated out as an OSS network entity. This entity is the AuC. The AuC database stores subscriber authentication keys. Other tasks carried out by the AuC include calculation of authentication parameters and then conveying these to the HLR.

Equipment Identity Register The equipment identity register (EIR) stores the international mobile equipment identity (IMEI) numbers for the entire network. The IMEI enables the MSC in identifying the type of terminal, mobile equipment manufacturer, and model and helps the network in locating the device in case it is stolen or misplaced. The EIR contains three different types of lists:

- A *black list* that includes mobile stations which have been reported stolen or are currently locked due to some reason
- A *white list* which records all MSs that are valid and operating
- A *grey list* including all those MSs that may not be functioning properly

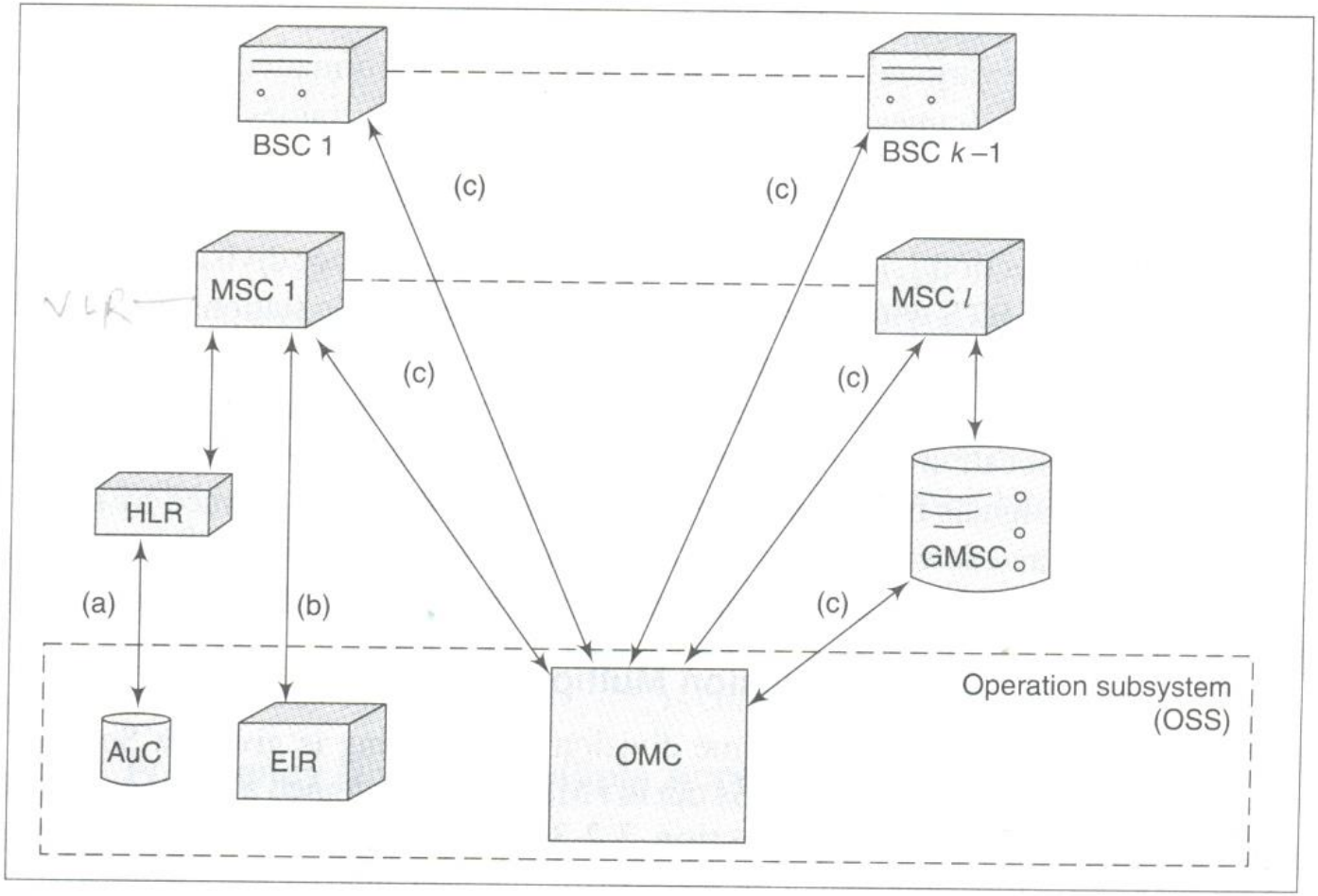


Fig. 3.9 OSS system architecture and connections between (a) AuC and HLR, (b) EIR and MSC, and (c) OMC and BSC, MSC, and GMSC

HANDOVER

3.6 Handover

Handover (also known as handoff as handover to one is handoff from another), to the neighbouring cell, is defined as a mechanism to hand over the control of a mobile device to the neighbouring cell (Section 1.7). This is, however, too simplistic a picture of the handoff–handover process. Handover is technically the process of transferring a call (or data transfer) in progress from one channel to another. The core network may perform handovers at various levels of the system architecture or it may hand over the call to another network altogether. There are two main reasons for handover in cellular networks—(a) if the mobile device moves out of the range of one cell (base station) and a different base station can provide it with a stronger signal, or (b) if all channels of one base station are busy, then a nearby base station can provide service to the device. The handover process is an important one in any cellular network. Also, the handover must be completed efficiently and without any inconvenience to the user. Different networks use different types of handover techniques. The following subsections describe the various types of handovers and the handover processes within GSM networks.

3.6.1 Types of Handover

Different cellular systems follow different regulations for handoff–handover processes. With the development of 3G standards and technology, it is possible for

several mobile phones to use the same channel and for neighbouring cells to use the same frequency bands. As a result of this, new handover methods have also evolved and are used in addition to the older techniques. The two main types of handover are *hard handover* and *soft handover*. These are discussed below.

3.6.1.1 Hard Handover

A hard handover is one where the existing radio link must be dropped for a small period of time before it can be taken over by another base station. In this type of handover, a call in progress is redirected not only from a base station to another base station but also from its current transmit–receive frequency pair to another frequency pair. An ongoing call cannot exchange data or voice for this duration. This break in call transmission is called call drop or call cut-off. Handover takes place in a few ms (at best in 60 ms) and the interruption is hardly discernible by the user. Handover to another cell is required when the signal strength is low and error rate is high. GSM systems perform hard handovers.

3.6.1.2 Soft Handover

3G CDMA systems have soft handover. Soft handover means an MS at the boundary of two adjacent cells does not suffer call drops due to handover in the boundary region. It gives seamless connectivity to an MS (Section 4.2.2.1). A method of soft handover that employs an offset to pseudo noise code is described in Section 4.2.2.2. Soft handover does not require breaking of the radio link for cell-to-cell transfer of a call. A mobile device can be connected to several base stations simultaneously.

HANDOVERS IN GSM

3.6.2 Handovers in GSM

Figure 3.15 shows the different kinds of handover when a mobile station MS_1 moves from one cell to another or when the traffic through a specific stage becomes very high. These types of handover are described in the following subsections.

3.6.2.1 Inter-cell Handover

SDMA by multiple antennae at the same BTS aligned in different directions results in the formation of multiple cells. Section 3.3 described how the signal measurements are continuously performed at the RRM (Figs 3.12 and 3.13) sublayers in the MS, BTS, and BSC. The RRM is also responsible for handover management. When the signal strength goes weak due to several reasons (for example, the MS moving away from the cell in which it is presently localized to the boundary region of another cell), there is handover from a cell to another. This process is called inter-cell handover. The signal strength changes inversely with the square of the distance from the transmitter. Therefore, as distance of the MS from a BTS in an i^{th} cell increases from s to $2s$, the signal strength decreases by factor of $(2s/s)^2 = 4$. Now, if the distance of the j^{th} cell decreases from $2s$ to s, the signal strength increases by a factor of 4. There is a boundary region where the signal quality improves and error rates decrease on handover.

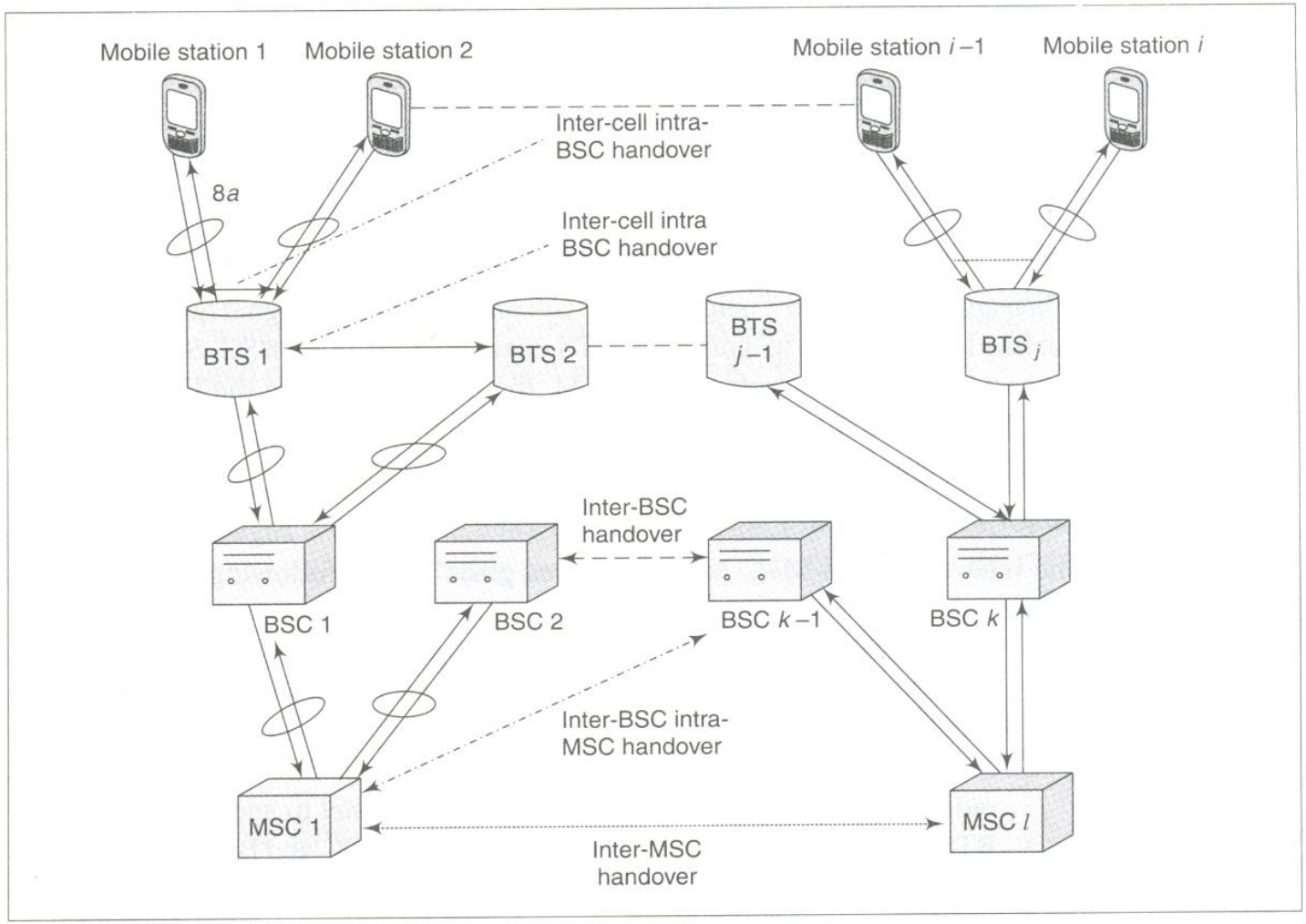


Fig. 3.15 Different kinds of handovers when a mobile station moves from one cell to another or when the traffic to a specific stage becomes too high

3.6.2.2 Inter-MSC Handover

Handover also takes place for load balancing when the traffic from the cells and BSCs is high. An ongoing call, which is being handled by a cell, may be handed over to another MSC. Since the two MSCs are interfaced through PCM (Fig. 3.14), the handover is performed over a wired line.

3.6.2.3 Inter-BSC Handover

Handover also takes place for load balancing when the traffic from the cells and BTSs is high. The BSCs connect to an MSC. A call, which is ongoing in a cell through a BTS, may be handed over to another BSC connected to the same MSC. Since the BSCs connect to the MSC interfaces by PCM, the handover is over a wired line.

3.6.2.4 Inter-BSC, Inter-MSC Handover

Handover also takes place for load balancing when the traffic from the cells and BTSs as well as the BSCs is high. The BTSs connect to a BSC and BSCs connect to

an MSC. A call, being handled by a cell through a BTS, may be handed over to another BSC connected to a different MSC.

3.6.2.5 Intra-cell Handover

Due to interference at certain frequencies, the signal quality becomes poor. The BSC can handover the call to another frequency of the cell in such cases.

3.6.2.6 Inter-cell, Intra-BSC Handover

When an MS moves to a neighbouring cell and suffers poor signal quality, the BSC can hand over the call to a different BTS channel of the same BSC. Since the BTSs connect to the BSC interfaced by PCM, the handover within the BTSs is over a wire but each BTS has different radio channels. The BSC, therefore, assigns a different radio channel (radio-carrier frequency).

3.6.2.7 Inter-cell, Intra-MSC Handover

The inter-cell, intra-MSC handover takes place by the following interchange of messages:

1. The RRM sublayer transmits a signal report from MS_i to BTS_i and from BTS_i to BSC_i. In case a handover is necessary, BSC_i signals the handover requirement to MSC_i.
2. MSC_i signals the handover requirement to another BSC_j and BSC_j allocates radio resources and transmits the activated channel to another BTS_k.
3. BTS_k sends acknowledgement of the channel to BSC_j and BSC_j acknowledges the handover request grant via a message to MSC_i.
4. MSC_i transmits handover command to BSC_i, in turn, BSC_i to BTS_i, and BTS_i to the MS_i's RRM layer. The RRM directs the MS radio interface to operate at another channel linked to BTS_k.

There is handover of the call to BTS_k and voice or data interchange starts through BTS_k.

New generation (2.5G) networks ensure mobility by handover not only among the BTSs, BSCs, or MSCs but also among the in-between LANs. This ensures seamless (uninterrupted) connectivity to the user.

SECURITY

3.7 Security

Being a wireless radio-based network system, GSM is quite sensitive to unauthorized use of resources. GSM networks employ various security features. Some of these security features are designed to protect subscriber privacy and certain other features are used to secure the network against misuse of resources by unregistered users. For example, to control access to the network, the MS is required to use a PIN before it can access the network through U_m interface (Section 3.1.2.1). This section provides a detailed discussion of GSM security features.

3.7.1 Authentication

As discussed in Section 3.1.2.3, the operation and maintenance subsystem of the GSM network has an AuC (authentication centre) for authenticating an MS. The AuC first authenticates the subscriber MS and only then does the MSC provide the switching service [this service enables the MS to switch (communicate) to another terminal TE, which is also authenticated in case it is an MS]. Authentication algorithms use a random number sent by the AuC during the connection setup and an authentication key which is already saved in the SIM. Authentication algorithms used can differ for different mobile service providers.

3.7.2 TMSI

When an MS moves to a new location area, the VLR (visitor location register) assigns a TMSI which is stored in the SIM of the MS. Therefore, the identification of the subscriber during communication is done using not the IMSI but the TMSI. This ensures anonymous call number identity transmission over the radio channels. (Caller line identification provision is a supplementary service. The VLR assigned TMSI generates that ID.) This protects the MS against eavesdropping from external sources. (IMSI of the MS is its public identity. TMSI is the identity granted on moving to a particular location.)

3.7.3 Encryption

The BTS and the MS have to perform ciphering before call initiation or before connecting for receiving a call (Section 3.5.4). The MS uses a cipher (encryption key) for encryption. The cipher is a result of performing mathematical operations on (a) the cipher key saved in the SIM, and (b) the cipher number received from the BTS when the call setup is initiated. The BTS transmits the cipher number before a call is set up or transmitted. The mathematical operations performed are in accordance with the algorithms employed by mobile service providers. Only encrypted voice and data traffic and control channel data is transmitted to the BTS. This makes wireless communication secure (confidential) between the MS and the BTS. The encryption algorithm is identical for all mobile service providers. This ensures compatibility between the BTS, BSC, and MSC units made by different manufacturers. The BTS deciphers the voice and data channel by running a deciphering algorithm before communicating over the wired PCM (pulse code modulation) lines.

The random numbers used in authentication and ciphering processes are also known as *challenge* to the mobile station to generate the results (responses) of the algorithms and only if these results are correct, do the BTS and other units grant access to the *challenged* MS.

MOBILE TCP

6.4 Mobile TCP

Mobile TCP (M-TCP) suggests the splitting of the TCP layer into two TCP sub-layers and a mechanism to reduce the window size to zero. The TCP split is asymmetric. The window is set to zero to prevent the transmission from the TCP transport layer at the MN or the fixed node, when disconnection is noticed. Disconnection is detected when the split connection does not get packets within a timeout interval. The window opens again on getting the packet. The M-TCP host at the base does not use slow start as it presumes that the packet loss is due to disconnection and not due to congestion or interference. Data flow control on the wireless part of the network is like an on–off control. The window size field is used for congestion control during transport. The window size field specifies the number of bytes the sender is willing to receive, starting from the acknowledgement field value. In slow start (Section 6.1.5), the window size is set to one at the beginning and on congestion detection. In M-TCP, it is set to zero on detection of packet loss or out of reach from the timeout or DACK from the other end.

Figure 6.8(a) shows the M-TCP supervisory host (SH_M) agent sub-layer between the base transceiver and the fixed node and conventional TCP between the fixed nodes.

One connection is between the MN and the BTS and the other between the BTS and the fixed node (FN). The BTS has an access point at an agent, SH_M for the TCP connection. SH_M sends and receives the packets to and from the MN through the BTS. M-TCP functions in the following manner:

1. SH_M sends and receives the packets to and from TCP_F layer at the fixed node. The transfer mechanism is simple. There is only one hop.

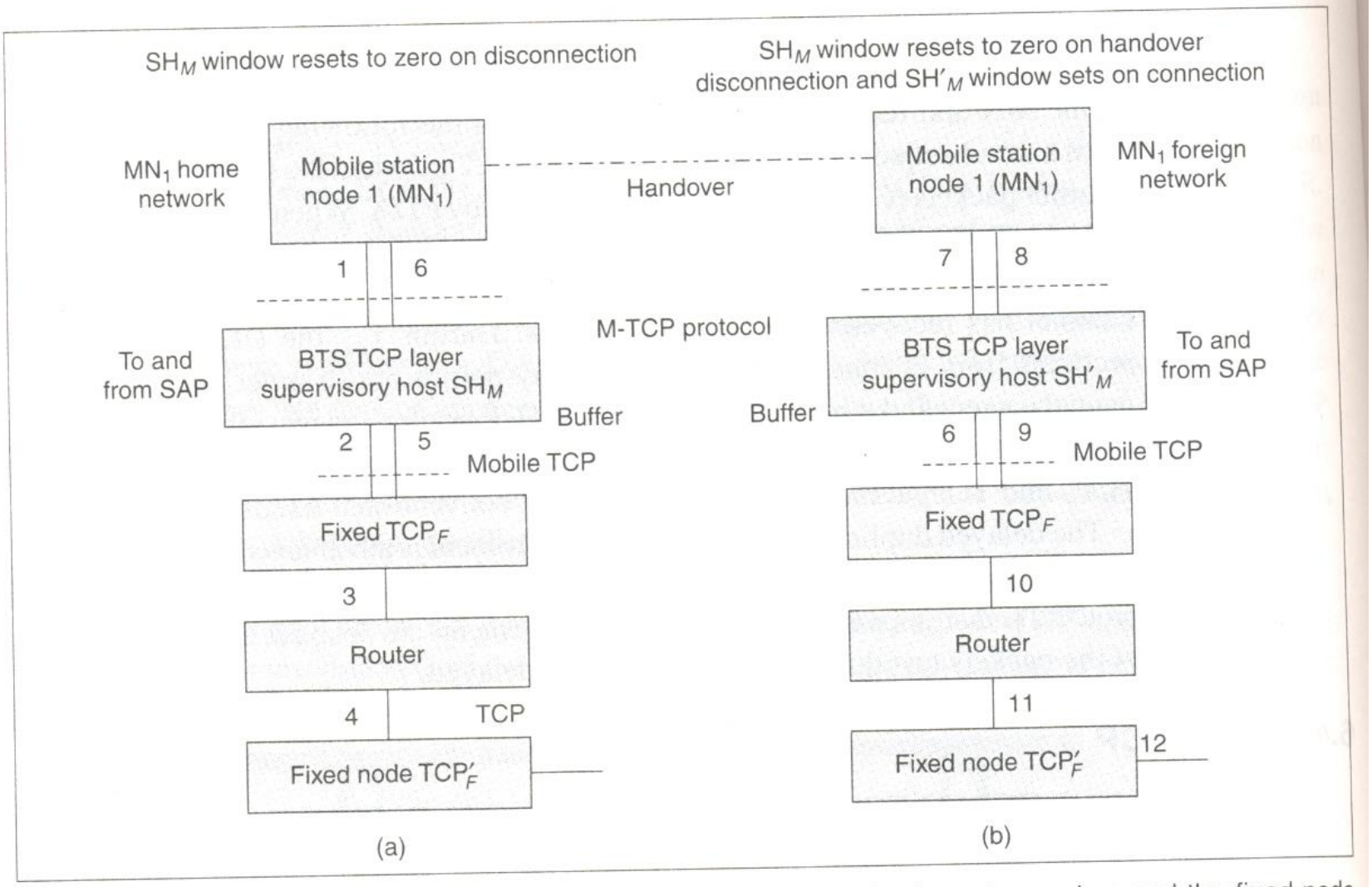


Fig. 6.8 (a) Mobile TCP supervisory host (SH_M) sub-layer between the base transceiver and the fixed node (with conventional TCP between the fixed nodes) (b) Handover mechanism

Retransmission of packets due to DAs between SH_M and TCP_F does not takes place, unlike the retransmission of packets between the fixed TCP nodes (Section 6.1.2). SH_M sets the window size to zero in case of timeout, as it presumes disconnection of the MN. The MN or TCP_F will also not retransmit as each of them finds that SH_M is not receiving packets within the timeout and has set the window to zero. When SH_M finds that the MN has sent the packet, it presumes that the connectivity is alive again and sets the window to its old value, i.e., the value when it last received the packets.

2. TCP_F layer at a fixed node sends and receives the packets to and from another fixed node TCP'_F. The transfer mechanism is standard, carried out by multiple hops through the routers.
3. Error detection and correction is done at the data link or physical layer at the BTS and the MN, not at SH_M.
4. The TCP header can be used during transmission between SH_M and the MN.

From the service access point (application) at the MN, data streams are received but not buffered at SH_M and, therefore, there is no retransmission from SH_M to the MN or to the fixed TCP_F layer. Figure 6.8(b) shows the handover mechanism.

SECURITY

10.8 Security

Section 1.8 described security. It is important for maintaining privacy and for mobile e-business transactions. Table 10.1 describes some of the security problems in mobile and wireless computing systems and Table 10.2 gives the solutions for such problems.

Table 10.1 Security problems in mobile and wireless computing systems

Security Problems	*Description*
Confidentiality	Only destined user must be able to read data. (Encryption of the data before transmission and deciphering it at the user end is a method employed for ensuring confidentiality.)
Integrity	Data integrity needs to be maintained or else the user receives a manipulated message. System integrity needs to be maintained or else system can issue the message to wrong node.
Pre-keying	In order to decipher the encrypted messages, a key for deciphering is first exchanged between transmitter and receiver. If a private key is used, key exchanges over wireless systems increase the risk of key trapping.
Availability	There may be a *denial of service* attack. A source can block the availability of data at the user end. For example, the packets sent can be prevented from reaching the destination by some intermediate router misdirecting them due to the attack.

(*Contd*)

(*Contd*)

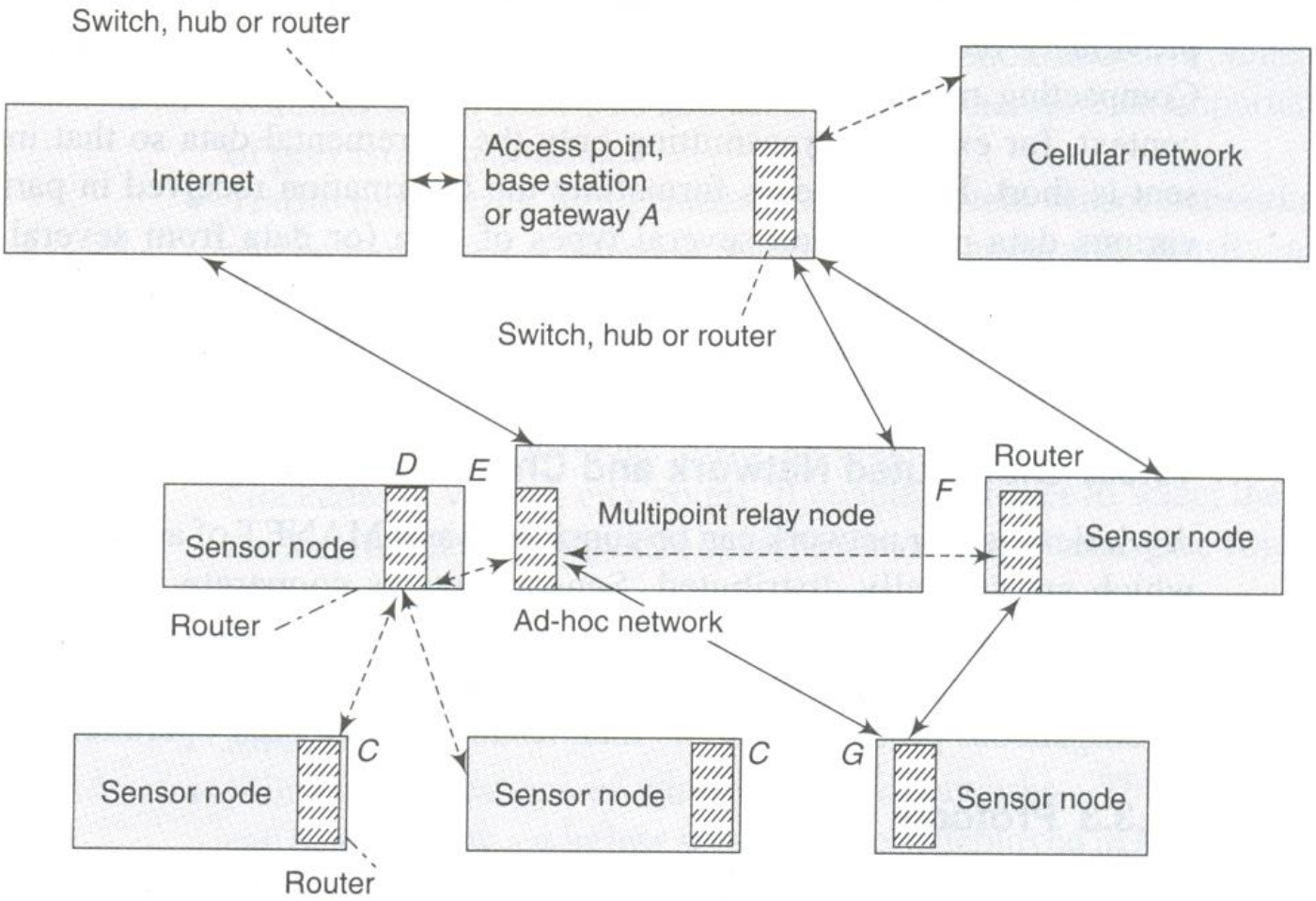
Non-repudiation	Non-repudiation means that a sender is unable to deny having sent a message or information. For example, if a user books an air ticket using a credit card and a mobile device, he is unable to deny this fact.
Resource constraint	Resource constraints of a mobile system include—(a) CPU runs at a slow speed compared to a conventional PC, (b) smaller memory availability, and (c) limited battery life. An attack form is exhausting of device-power by forcing it to transmit or receive data continuously or exhaustion of device-memory due to caching and hoarding irrelevant data from the attacker. Such an attack if occurs in between routers in the network, it seriously affects the whole network.
Power of detection	A mobile device may not detect the signals and therefore get data or message due to attack by jamming signals (A solution is Frequency hopping of the modulation signal which has high background noise.)
Interception	The interception of the signals (CDMA FHSS can be a solution to this problem.)
Replay	After studying the authentication requests and the client responses, attacker can replay the same sequence repeatedly.
Stealing of the subscribed service	Hijacking of user name and password by an attacker results in getting a service subscribed by another client.
Mobility risks	Changed location results in signals routing through paths, which cannot be relied upon.
Spoofing (impersonating address)	A node can impersonate an address in a mobile ad hoc network (Sections 1.5.3, 11.1, and 11.2). A common node to several paths can lead to choking of all routes.
Reconfiguration	An attack can be network configuration (e.g., manipulation of routing table). Network reconfiguration at different periods prevents such attacks.
Eavesdropping	Unsolicited messages from another source during a talk between two sources is called eavesdropping.
Traffic analysis	A security attack can occur by extracting information form the analysis of network traffic.

Table 10.2 Solutions for the security problems in mobile and wireless computing systems

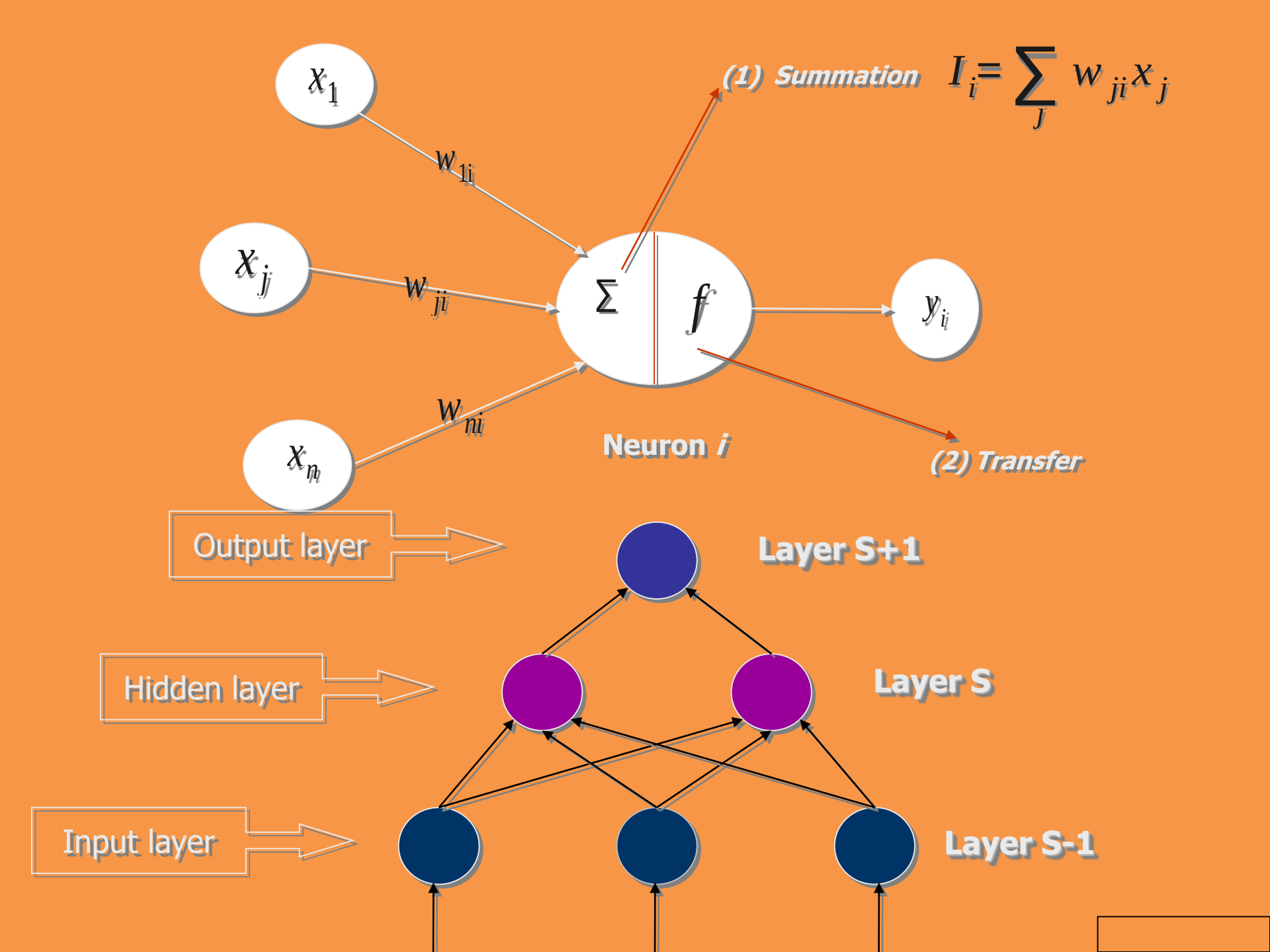
Solution	*Description*
Direct signalling with restricted signal strengths	Using the directed signals with the signal strengths set such that these are just sufficient to reach and detected successfully to reduce security risks from other directions as well as sources at farther distances in the same direction.
Hardware technique	FHSS is an example in which hardware is used for reducing security risks.
Hash	The hash of a message is a set of bits obtained after applying the hash algorithm (or function). This set of bits is altered in case the data is modified during transmission. It checks data integrity.
MAC	MAC (Message authentication code) is a combination of hash and secret key.
Encryption	Public key and private key encryptions—DES, AES, and RSA cryptographic algorithms (Table 1.5).
SSL	Secure socket layer (SSL) is a protocol that runs between HTTP and TCP (application and transport layer protocols) for secure transactions between client and Web server. The protocol HTTP + SSL is called HTTPS and the website address now starts with www.https://. The sub layers of SSL are handshake and record protocols. Handshake protocol authenticates both client and server and allows both of them to negotiate the data security protocols to be used later. The record protocol transfers the payload. SSL supports (i) hash function MD5 (message-digest algorithm 5) and SHA (secure hash algorithm), (ii) digital signatures, (iii) RSA and DES , (iv) MAC (medium access control) on SHA and MD5, (v) data encryption algorithms—DES and triple DES, and other encryptions.
Checksum or Parity	Checksum and parity are the primitive methods to check message integrity.
IPSec	IPSec (Internet protocol for security) protocols (i) Authentication Header (AH) is a method for message integrity check. (ii) ESP (Encapsulating Security Payload) is a protocol for confidentiality. (iii) Internet Key Exchange (IKE) protocol to exchange the authentication keys with protection.
CHAP	CHAP (challenge handshake authentication protocol) is a method for authentication of point-to-point communication.
RADIUS	RADIUS (remote authentication dial in user service) is a service for sending the message that the client stands authenticated.
AAA	AAA (authentication, authorization, and auditing) is a strategy for security.

(*Contd*)

(*Contd*)



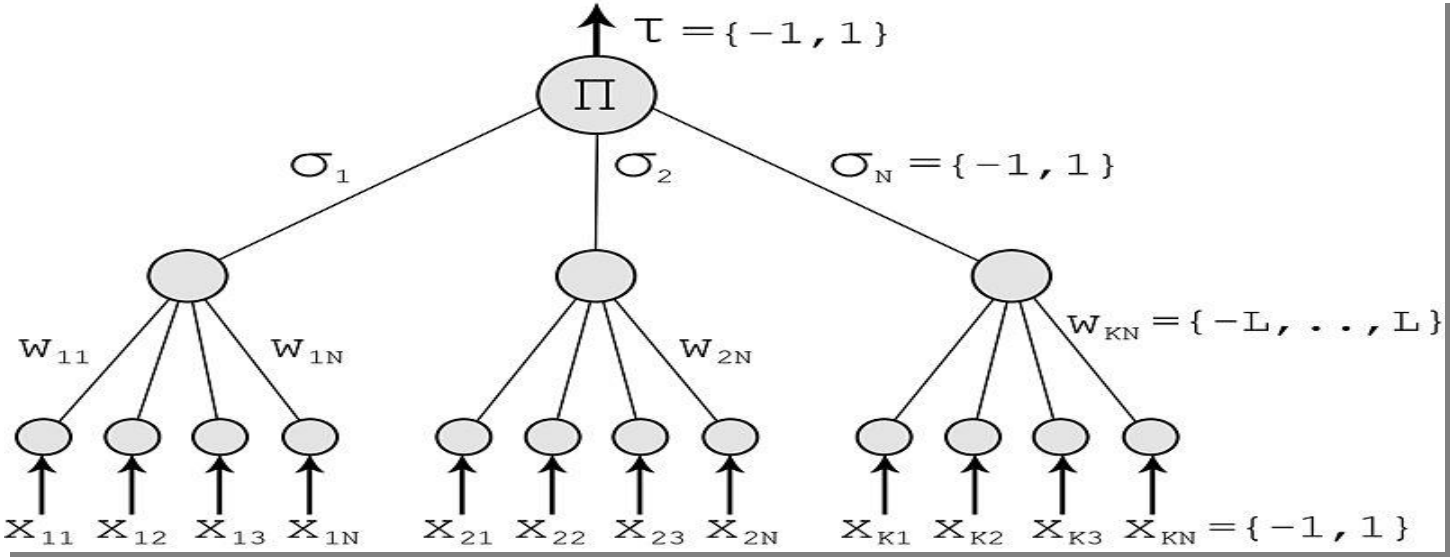
g. 11.3 Wireless sensor network


x_1
x_j
x_n
w_{1i}
w_{ji}
w_{ni}
Σ
f
y_i
(1) Summation
$I_i = \sum_j w_{ji} x_j$
(2) Transfer
Neuron i
Output layer
Hidden layer
Input layer
Layer S+1
Layer S
Layer S-1

Key Generation using Neural Network

Tree Parity Machines

Tree Parity Machines, which are used by partners and attackers in neural cryptography,are multi-layer feed-forward networks.



K - the number of hidden neurons,

N - the number of input neurons connected to each hidden neuron, total (K*N) input neurons.

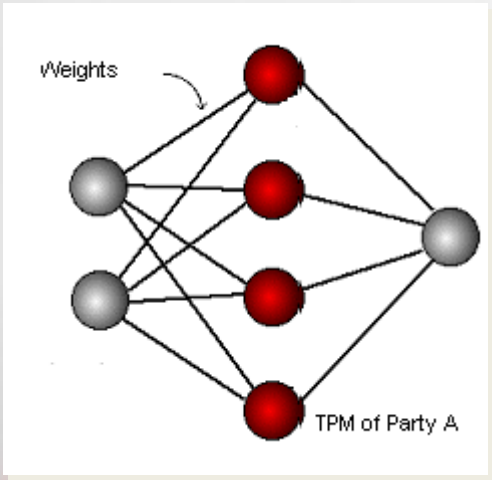
L - the maximum value for weight {-L..+L}

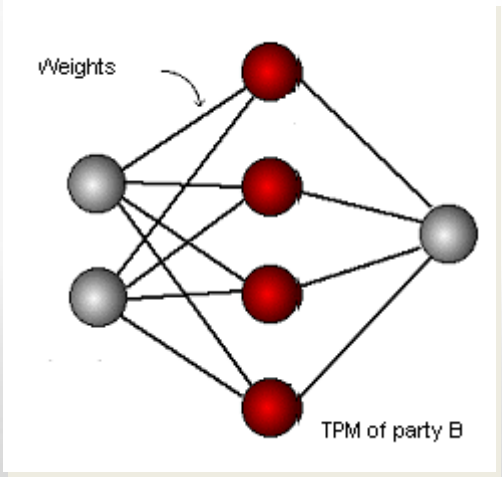
Here K = 3 and N = 4.

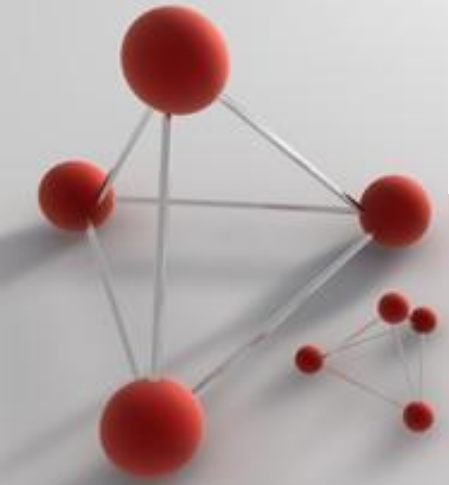
Neural Synchronization Scheme

Each party (A and B) uses its own (Same) tree parity machine.
Synchronization of the tree parity machines is achieved in these steps

1. Initialize random weight values





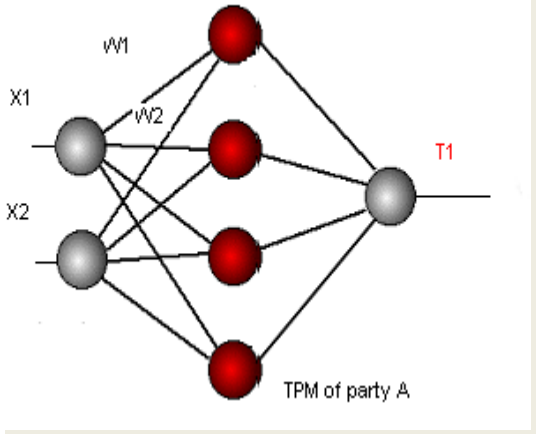


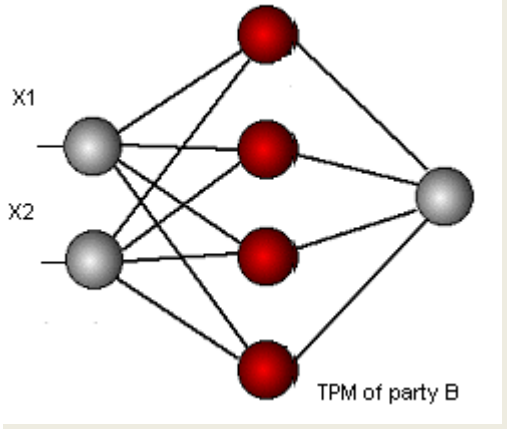
Neural Synchronization Scheme

2. Execute these steps until the full synchronization is achieved

2.1. Generate random input vector X

$$x_{ij} \in \{-1, +1\}$$





2.2. Compute the values of the hidden neurons

$$\sigma_i = \operatorname{sgn}\left(\sum_{j=1}^{N} w_{ij} x_{ij}\right)$$

Signum is a simple function, which returns -1,0 or 1:

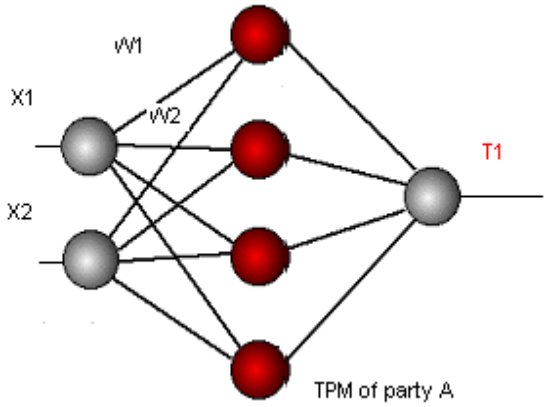
$$\operatorname{sgn}(x) = \begin{cases} -1 & \text{if } x < 0, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x > 0. \end{cases}$$

Neural Synchronization Scheme

2.3. Compute the value of the output neuron

$$\tau = \prod_{i=1}^{K} \text{SIGN}\left[\sum_{j=1}^{N} w_{i,j}\, x_{i,j}\right]$$

2.4. Compare the values of both tree parity machines



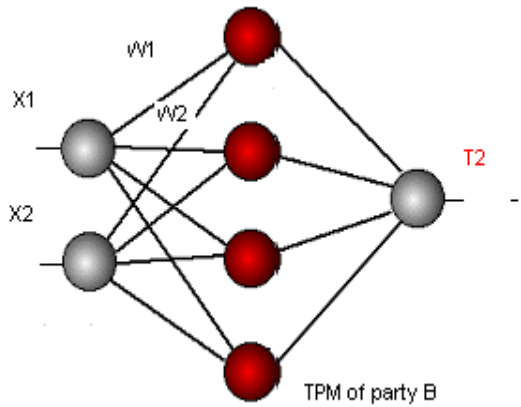
2.4.1 Outputs are others: go to 2.1

Output(A) ≠ Output(B)

2.4.2 Outputs are same:

Output(A) = Output(B)

one of the suitable learning rules is applied to the weights



How do we update the weights?

We update the weights only if the final output values of the neural machines are equal.

One of the following learning rules can be used for the synchronization:

- Hebbian learning rule:

$$w_i^+ = w_i + \sigma_i x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

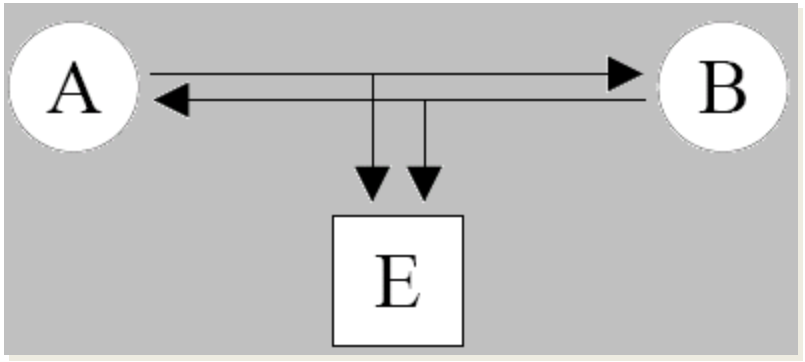
- Anti-Hebbian learning rule:

$$w_i^+ = w_i - \sigma_i x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

- Random walk:

$$w_i^+ = w_i + x_i \Theta(\sigma_i \tau) \Theta(\tau^A \tau^B)$$

Learning with own tree parity machine



In each step there are 3 situations possible:

1. **Output(A) ≠ Output(B):** None of the parties updates its weights.
2. **Output(A) = Output(B) = Output(E):** All the three parties update weights in their tree parity machines.
3. **Output(A) = Output(B) ≠ Output(E):** Parties A and B update their tree parity machines, but the attacker can not do that. Because of this situation his learning is slower than the synchronization of parties A and B.

Cycle Formation of key

The synchronized weight vector from the previous phase in the form of blocks of bits with different size like 8/ 16/32/ 64/ 128/ 256. The rules to be followed for generating a cycle are as follows:

	1st half Weight Vector Block				2nd half Weight Vector Block			
	(MSB)			(LSB)	(MSB)			(LSB)
Sender's steps	S= 0	1	0	1	0	0	1	1
	K= 1			*0*	*1*			*0*
	I1= 1	1	0	1	1	0	1	1
	K=	*0*	*1*			*0*	*1*	
	I2= 1	1	1	1	1	0	0	1
Receiver's steps	*K= 1*			*0*	*1*			*0*
	I3= 0	1	1	1	0	0	0	1
	K=	*0*	*1*			*0*	*1*	
	I4= 0	1	0	1	0	0	1	1

Final Step of Encryption

For different size of weight sub vector different intermediate blocks may be considered as the corresponding encrypted blocks. For example, the policy may be something like that out of three weight sub vector blocks B_1, B_2, B_3 in a key block of bits, the 4^{th}, the 7^{th} and the 5^{th} intermediate blocks respectively are being considered as the final key blocks. In such a case, the key of the scheme will become much more complex, which in turn will ensure better security.

Final Neural Key Block=Intermediate Weight Vector Block of cycle

+

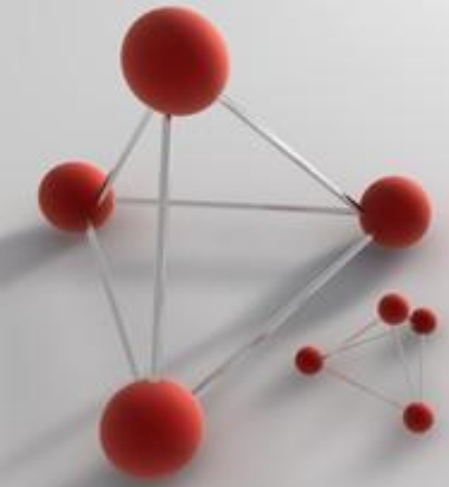
Position information of Intermediate Weight Vector Block of cycle

Now perform cascading xoring of Modulo2 encrypted block with the Neural Secret Key, final encrypted cipher text is generated. This stream of bits, in the form of a stream of characters, is transmitted as the encrypted message.

Results

The results have been presented on the basis of the following factors:

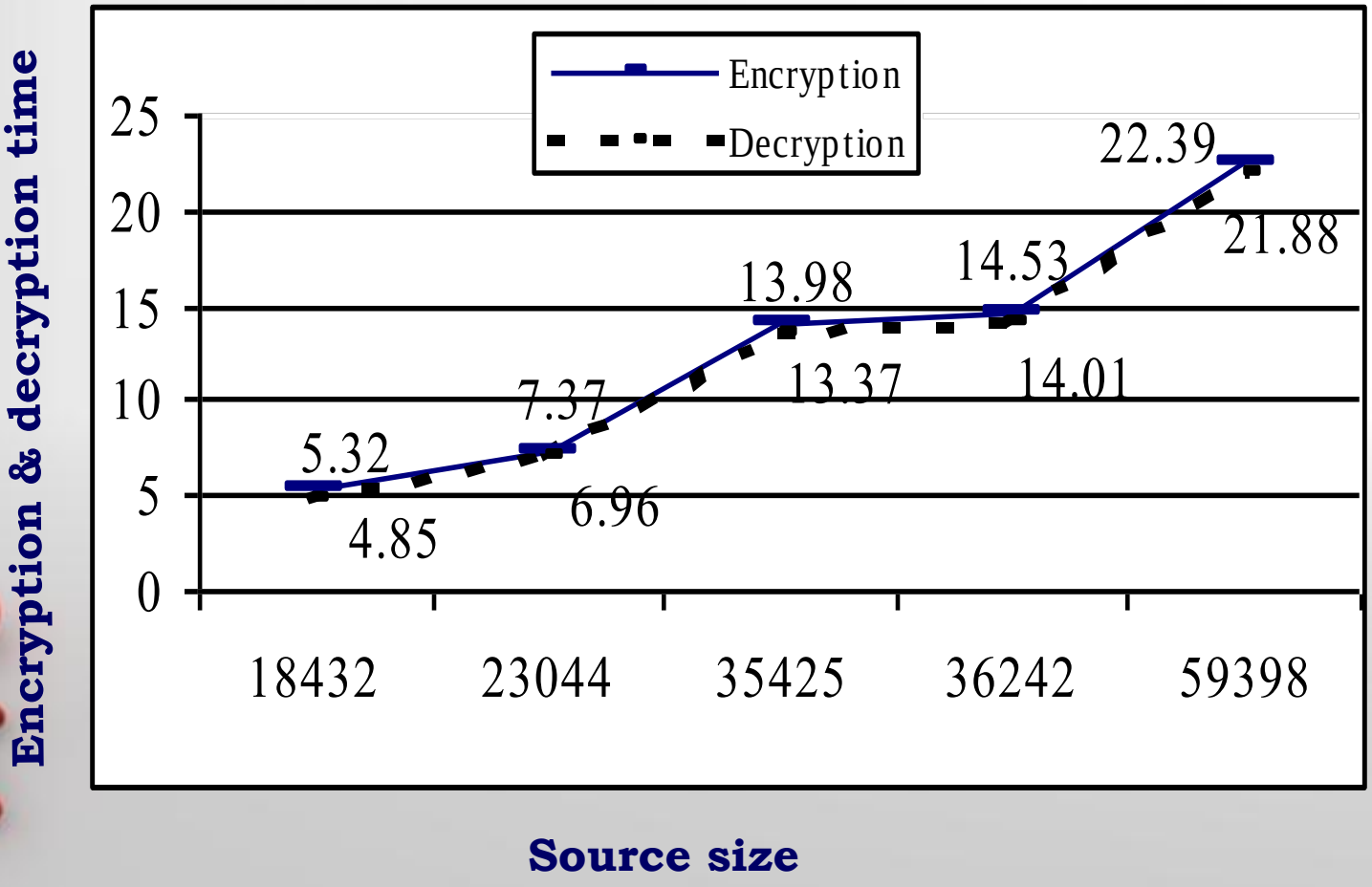
- Computation of the encryption time, the decryption time, and the Pearsonian Chi Square value between the source and the encrypted files
- Performing the frequency distribution test
- Comparison with the RSA technique



Encryption/decryption time Vs. File size

Encryption Time (s)			Decryption Time (s)		
Source Size (bytes)	**Proposed ANNRPMS**	**RPSP**	**Encrypted Size (bytes)**	**Proposed ANNRPMS**	**RPSP**
18432	**5. 32**	7.85	18432	**4.85**	7.81
23044	**7. 37**	10.32	23040	**6.96**	9.92
35425	**13. 98**	15.21	35425	**13. 37**	14.93
36242	**14. 53**	15.34	36242	**14. 01**	15.24
59398	**22. 39**	25.49	59398	**21. 88**	24.95

Source size Vs. encryption time & decryption time

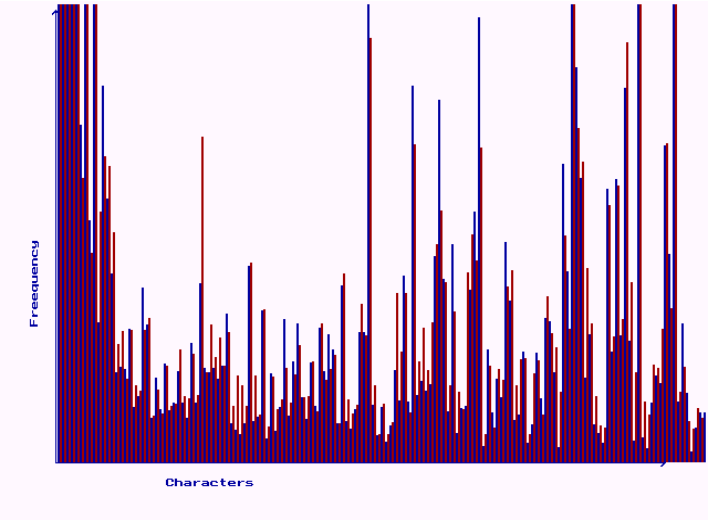


Source size Vs.Chi-square value

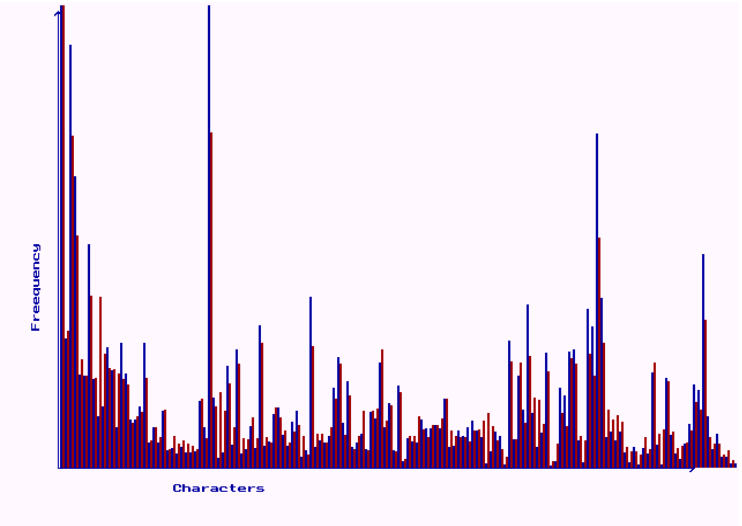
Stream Size (bytes)	Chi-Square value (TDES)	Chi-Square value (Proposed ANNRPMS)	Chi-Square value (RBCM CPCC)	Chi-Square value (RSA)
1500	1228.5803	2465.0645	2464.0324	5623.14
2500	2948.2285	5643.4673	5642.5835	22638.99
3000	3679.0432	6757.1533	6714.6741	12800.355
3250	4228.2119	6996.6177	6994.6189	15097.77
3500	4242.9165	10572.6982	10570.4671	15284.728

Results for Frequency Distribution Test

Frequency Distribution Chart for Source file and Encrypted file



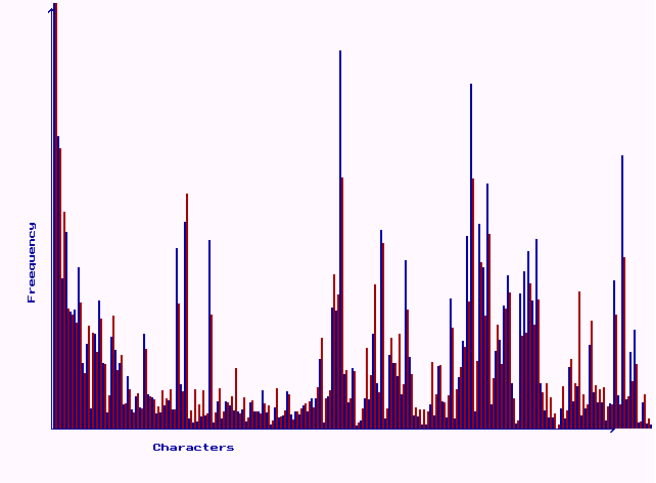
Segment of Frequency Distribution Chart for ANNRBLC.EXE and Encrypted A1.EXE



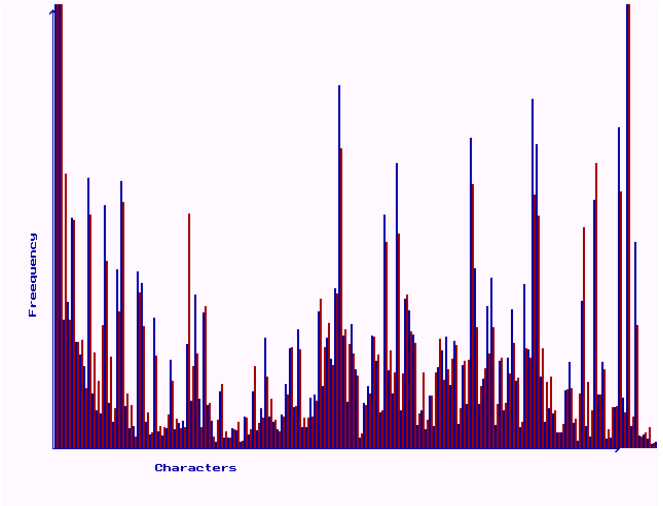
Segment of Frequency Distribution Chart for DOSKEY.COM and Encrypted A3.COM

Blue lines indicate the occurrences of characters in the source file and red lines indicate the same in the corresponding encrypted file

Frequency Distribution Chart for Source file and Encrypted file



Segment of Frequency Distribution Chart for NDDEAPI.DLL and Encrypted A2.DLL

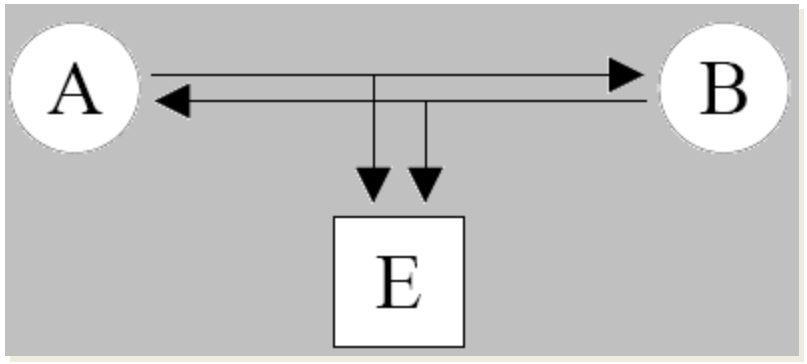


Segment of Frequency Distribution Chart for USBD.SYS and Encrypted A2.SYS

Blue lines indicate the occurrences of characters in the source file and red lines indicate the same in the corresponding encrypted file

Cryptanalysis

Attacks and security of this protocol



Key exchange between two partners with a passive attacker listening to the communication.

In every attack it is considered, that the attacker E can eavesdrop messages between the parties A and B, but does not have an opportunity to change them.

Brute force

To provide a brute force attack, an attacker has to test all possible keys (all possible values of weights Wij). By K hidden neurons, K*N input neurons and boundary of weights L, this gives $(2L+1)^{KN}$ ***possibilities. For example, the configuration K = 3,L = 3 and N = 100 gives us*** $3*10^{253}$ ***key possibilities, making the attack difficult.***

Secure Data Communication in Mobile Ad Hoc Networks

Goal

- “Secure data transmission”
- Provide an end-to-end protocol that:
  - works with TCP
  - provides data integrity
  - provides message authentication
  - provides replay protection
  - detects and compensates for path disruption

Assumptions

- All network nodes have:
  - unique identity
  - public/private key pair
  - module implementing network protocols
  - module providing communication across wireless network interface

Assumptions

- Any two nodes can establish an end-to-end Security Association, instantiated by a symmetric shared key, at the time of initial route discovery
- Any intermediate node that does not behave correctly is an adversary
- Multiple paths are node-disjoint
- Route discovery is secure

Secure Message Transmission (SMT) Protocol

- A node, S, establishes a secure association with another node, T
- S has a set of discovered, active, node disjoint paths through which it can communicate with T
- S uses message dispersion and encryption to add redundancy to a message it wishes to send to T

SMT - Continued

- S then “breaks” the message into N pieces, M of which need to reach T intact in order for T to recover the message
- Each piece of the message has a message authentication code and a sequence number, so that T can verify the validity of the message pieces and reject replays

SMT - Continued

- T sends to S a feedback message (like an ACK) for each successfully received piece
- S validates the feedback messages or receives a timeout when no feedback messages are received
- Each time a message piece is received or not received, the route rating for its route is updated (increased or decreased)
  - Route ratings indicate how preferable a route is, if it is failed or active, and its probabilistically calculated survival time.

Secure Single Path (SSP) Protocol

- Just like SMT, except -
  - Does not perform data dispersion
  - Uses only one path per message
- Lower transmission overhead than SMT
- Higher potential delay time than SMT

How it Works: Path Discovery

- Paths discovery can be implicit or explicit
  - Explicit allows SMT additional versatility and robustness, because it can compose routes from the discovered routes and can correlate loss/delivery with specific links
- Assumed to be secure
  - Secure Routing Protocol, as proposed by the authors, or
  - paper references [2], [3], [4], [5], [6], and [39] all provide proposals for secure route determination protocols or for securing existing route determination protocols

How it Works: Path Rating

$$r_s(0) = \delta(r_s^{\max} - r_s^{\text{thr}}),\ 0 < \delta < 1$$

$$r_s(i) = \begin{cases} \max\left\{r_s(i-1) - \alpha, r_s^{\text{thr}}\right\}, & \text{if loss} \\ \min\left\{r_s(i-1) + \beta, r_s^{\max}\right\}, & \text{if success} \end{cases}$$

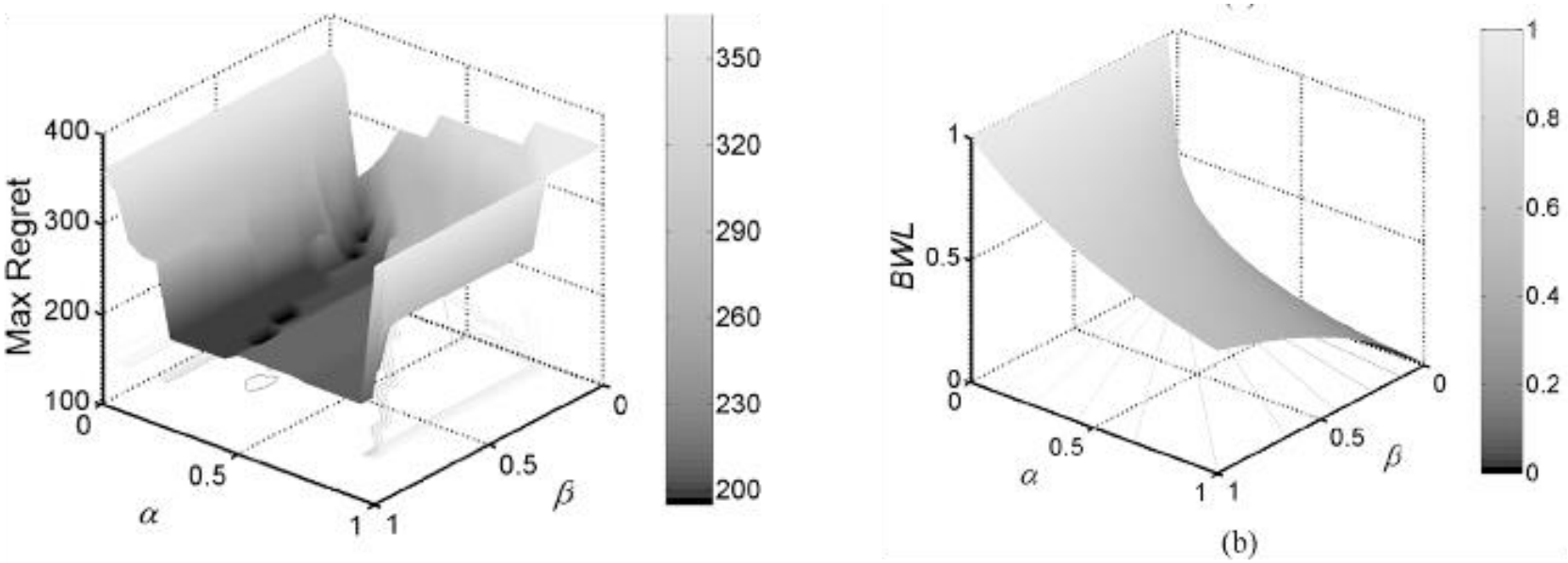
i : transmission number

r_s : rating of path, s

r_s^{thr} : minimum possible rating

$r_s^{\max}$: maximum possible rating

How it Works: Choosing α and β



Minimise Regret and Bandwidth Loss (BWL)

How it Works: Path Survival

$$\hat{p}_i(t) = \begin{cases} \frac{(s-1)}{s}, & \text{if } t + d < \tau_1 \\ \frac{(s-j)}{s}, & \text{for } j \text{ s.t. } \tau_j \leq t + d < \tau_{j+1} \\ \frac{1}{s}, & \text{if } t + d > \tau_s \end{cases}$$

S: number of Samples

t: current path age

d: maximum transmission time

τ: lifetime of route

How it Works: Configuration Algorithm

- Inputs:
  - path set
  - path ratings
  - path survival probabilities
  - optimization objective (successful transmission, minimal transmission overhead)
  - objective specific parameter (desired probability of successful transmission or maximum redundancy)

How it Works: Configuration Algorithm II

- All paths ranked
  - path rating, highest to lowest
    - survival probability, highest to lowest
      - number of hops, lowest to highest
- For all paths and redundancy options, the probability of successful transmission is calculated
- Result is an M by N matrix
- Search matrix to determine (M,N) values that satisfy the input objective

How it Works: Meeting Input Objectives

$$P_{\mathrm{GOAL}} - N_{\min}: \min_{\substack{1 \le N \le k \\ 1 \le M \le N}} \{N | R(M,N) \ge P_{\mathrm{GOAL}}\}$$

Find the minimum number of paths to achieve a certain success probability

$$P_{\mathrm{GOAL}} - r_{\min}: \min_{\substack{1 \le N \le k \\ 1 \le M \le N}} \{\bar{r} | R(M,N) \ge P_{\mathrm{GOAL}}\}$$

Find the minimum redundancy to achieve a certain success probability

$$r_{\mathrm{GOAL}}: \max_{\substack{1 \le N \le k \\ 1 \le M \le N}} \{\bar{R}(M,N) | \bar{r} \le r_{\mathrm{GOAL}}\}$$

Find the best values of M and N to achieve the highest probability of success given a certain redundancy

Simulation Details

- OPNET - commercially available network simulation software. Free for university courses or R&D
  - network area of 1000m2
  - 3 message sources, 4 - 512B messages each
  - 900s per simulation; 30 randomly seeded runs

Simulation Details

- 50 identical nodes
  - 300m communications range
  - 5.5 Mb/sec data rate
  - 655kB MAC buffer
  - Random Waypoint Mobility, 1m/s - 20m/s

Protocol Parameters

$P_{\mathrm{GOAL}} = 0.95$: specified probability of success

$r_s^{\mathrm{thr}} = 0.0$: minimum path rating

$r_s^{\mathrm{max}} = 1.0$: maximum path rating

$\alpha = 0.33$: rating decrease if loss

$\beta = 0.033$: rating increase if success

$\delta = 0.75$: initial path rating

Adversaries drop packets in both directions

No significant difference if drop packets or corrupt

Simulated Protocols

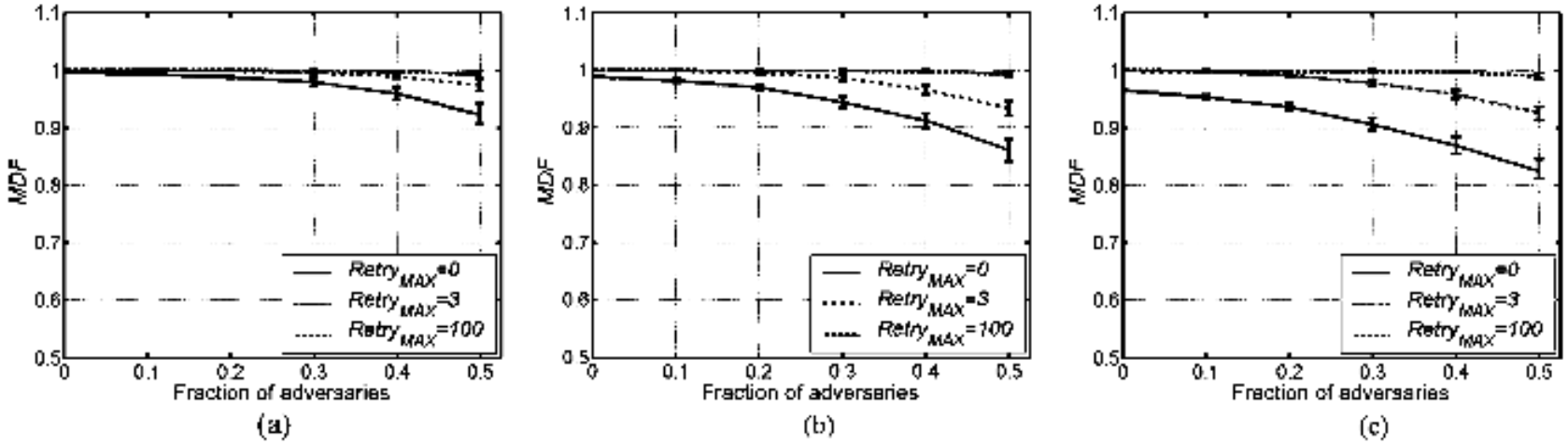
- SMT-LS
  - SMT with Link State
  - Idealised routing discovery scheme
    - no delay
    - no control overhead

Simulated Protocols

- SMT-RRD
  - SMT with Reactive Route Discovery
  - SMT integrated with Secure Routing Protocol
- SSP
  - SSP integrated with Secure Routing Protocol

Simulation: Reliability

Message Delivery Fraction



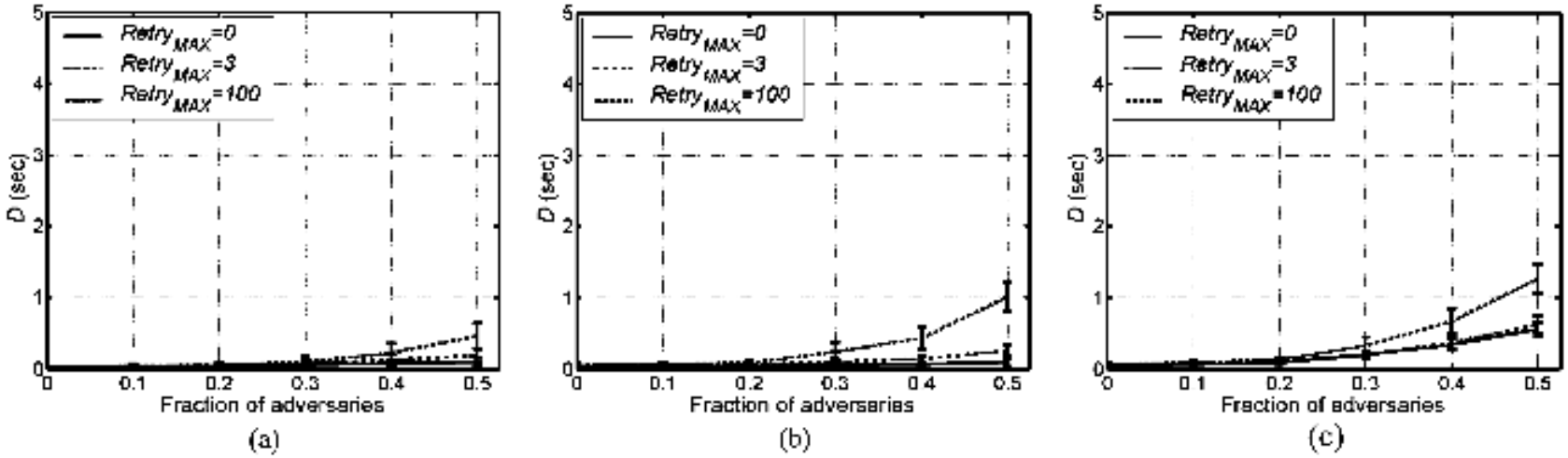
SMT-LS **SMT-RRD** **SSP**

Note: Messages with delay > 30s were ignored

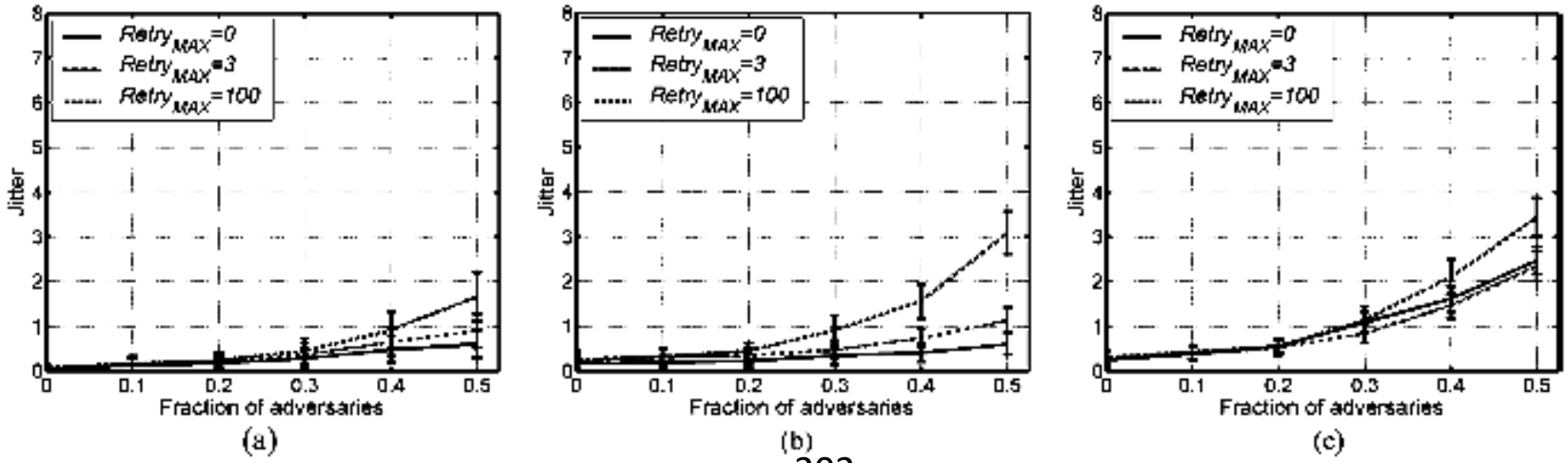
Up to 0.7% of the messages sent are not accounted for

Should these messages be counted as lost?

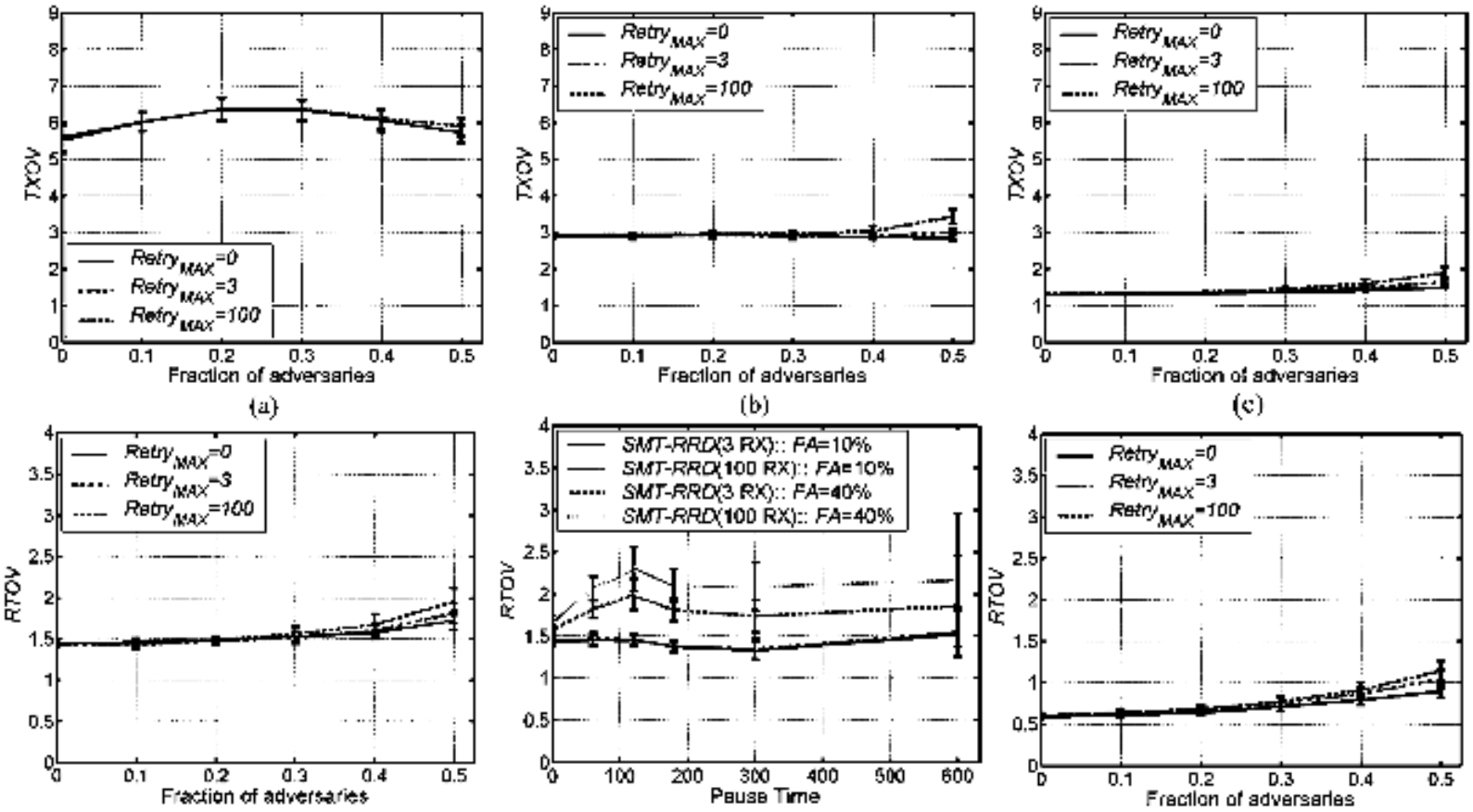
Simulation: Delay



SMT-LS **SMT-RRD** **SSP**

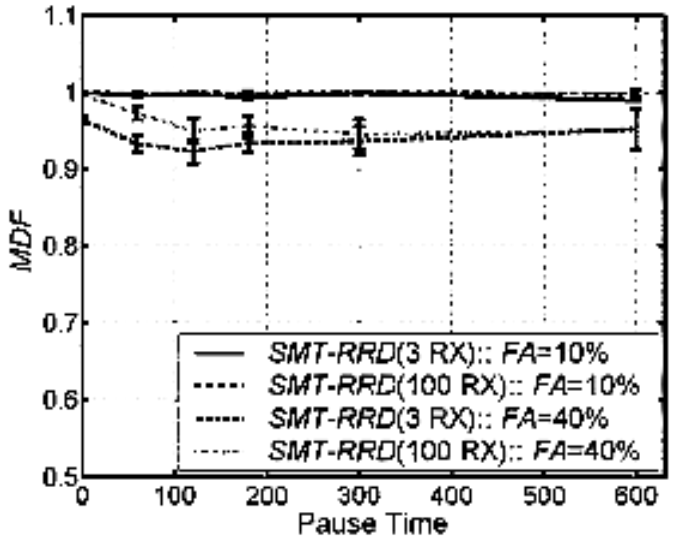


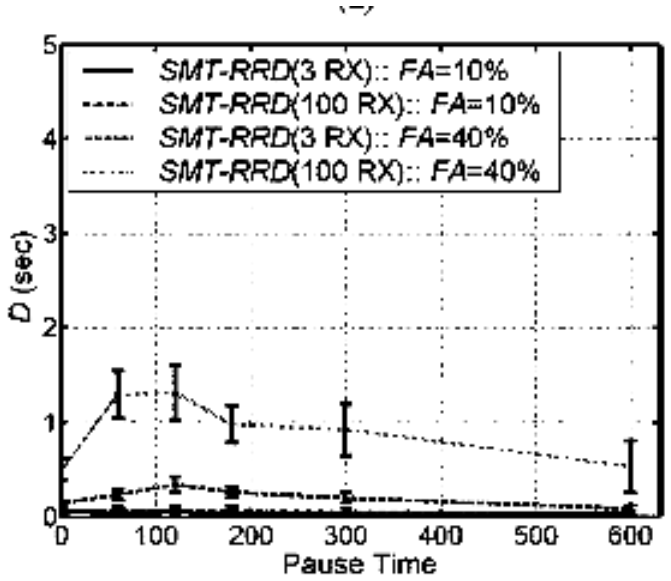
Simulation: Overhead Transmission and Routing



SMT-LS **SMT-RRD** **SSP**

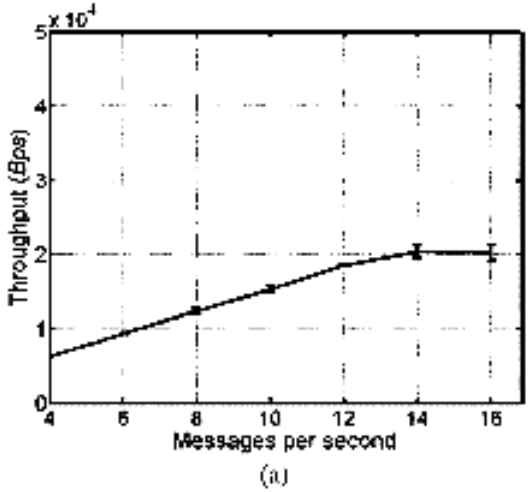
Simulation: Mobility

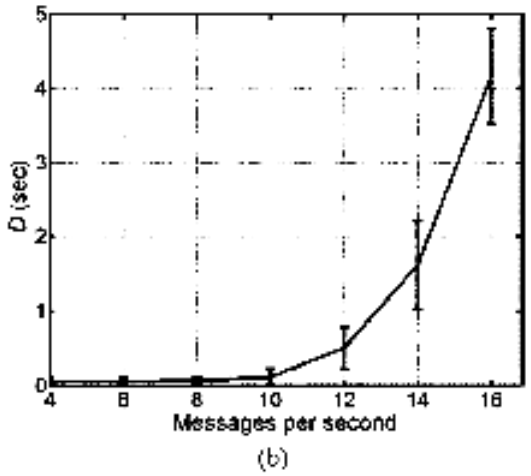


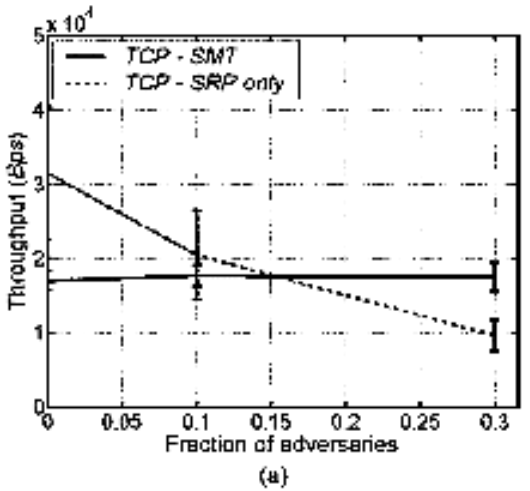


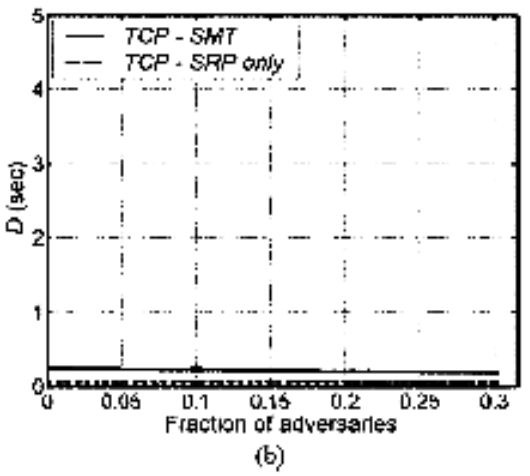
Pause Time: How long does the node stay in one place?
Larger pause time ⇒ less mobility

Simulation: Network Load





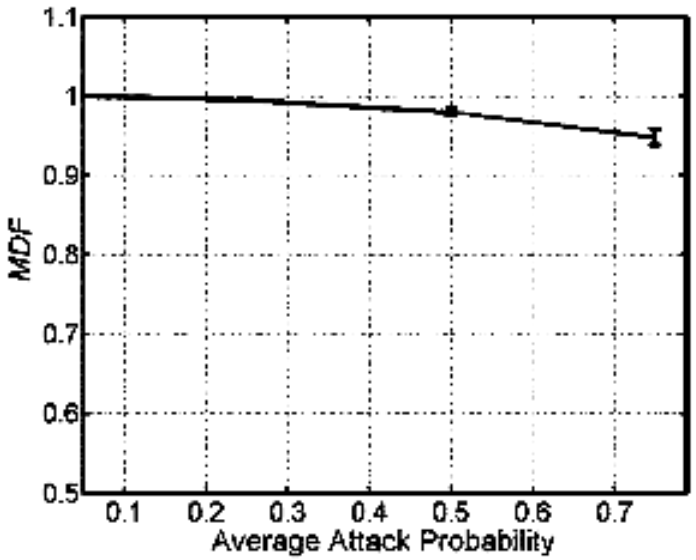


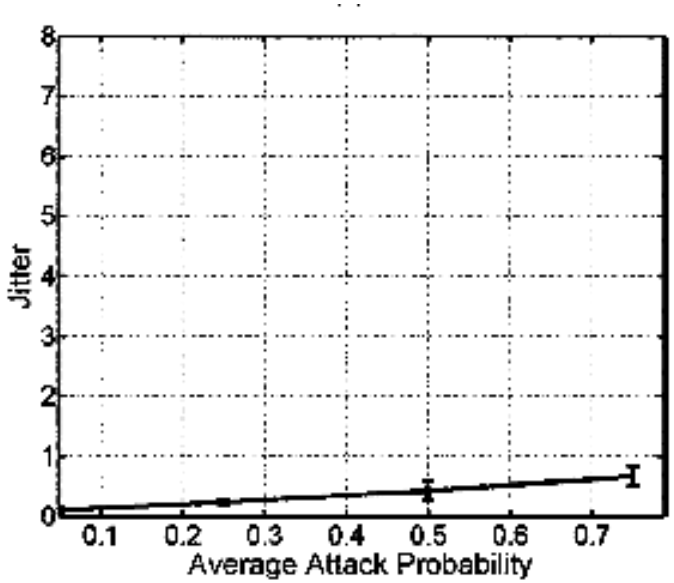


SMT-RRD, CBR

TCP

Simulation: Attack Resistance





FA: 50%

$$(\alpha, \beta) = (0.3, 0.05)$$

$$\text{Retry}_{\text{MAX}} = 3$$

Conclusions

- Provides end-to-end security
  - Effectively protects against data loss
  - Requires no advance knowledge of node trustworthiness
  - Automatically adapt to environment
  - Mechanism not subject to abuse by adversaries
- Tactical systems that operate in hostile environments
- Civilian systems compromised by selfish users and rogue network devices

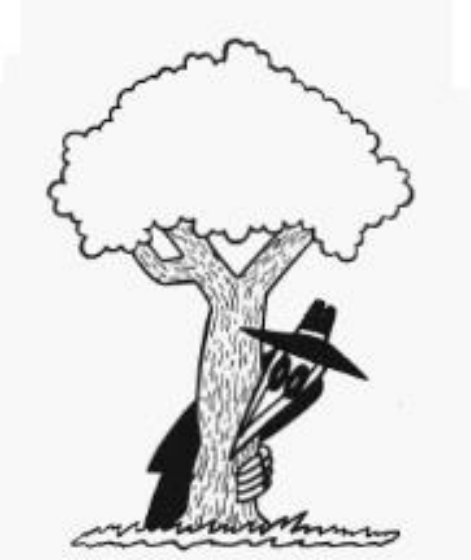
Security for Telecommuting and Broadband Communications

New NIST Recommendation

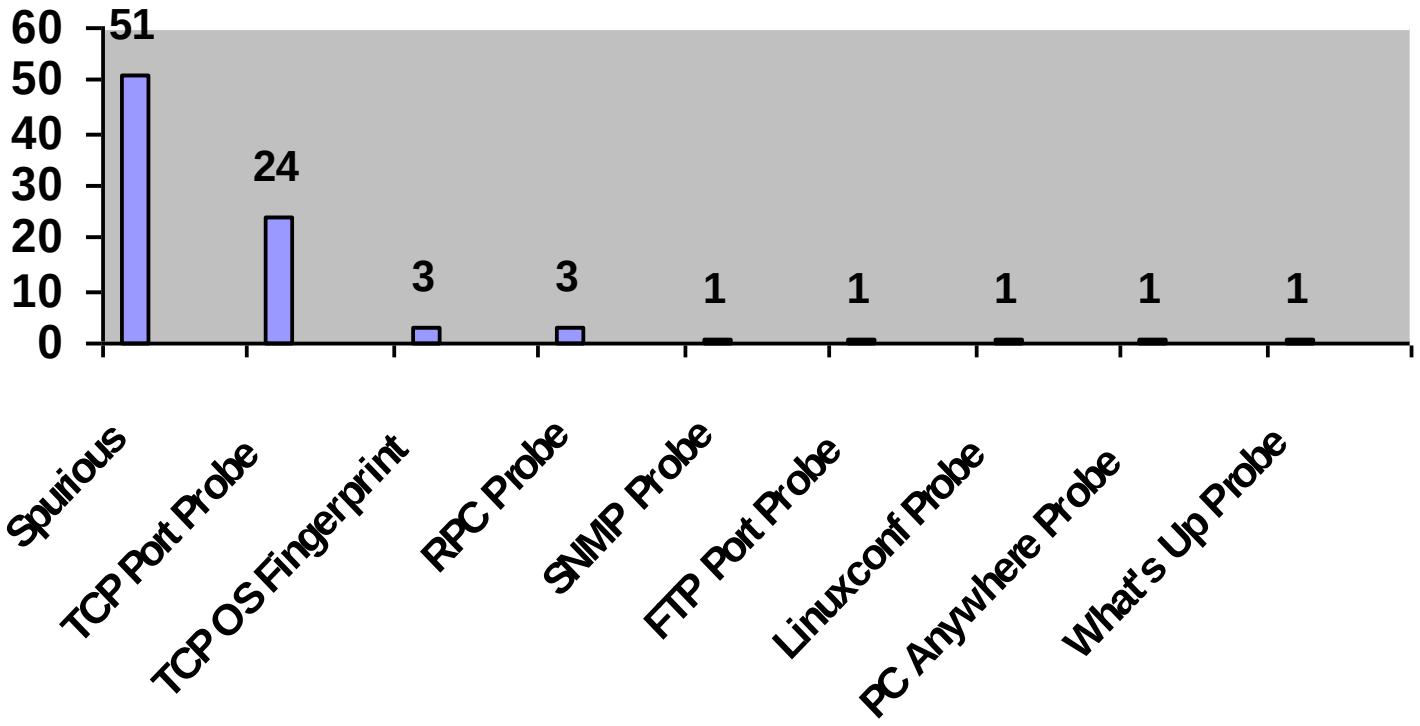
- For users, system managers, and agency administrators
- Step-by-step instructions on
  - Personal firewalls
  - Securing web browsers
  - Securing PC configurations
  - Home networking
  - Virtual private networks
  - Telecommuting architectures
  - Agency/enterprise considerations

What's different about broadband?

- Always on
  - Longer exposure to internet
  - User less likely to notice attack
  - May be permanent IP address
- Higher speed
  - Downloads of malicious code faster, less noticeable
  - Faster probes for vulnerabilities



10-Day Record of Intrusion Attempts



Personal firewalls

- First line of defense
- Estimates are more than 90% of home PCs have some vulnerability to Internet
- Good software firewalls available at low or no cost (examples listed in document)
- Stand-alone firewalls for home machines very cheap – under $100

Firewalls

- **Establishing a secure firewall configuration** – explains how to set up firewall
- **Running an online security assessment** – free scanners listed
- **Firewall features** – lots of variation among products

Firewalls – What to Look For

- **Logging** – track IP address of suspicious packets, some let you find out where packets from (‘whois’)
- **Port hiding** – does not respond to unsolicited contacts
- **Automatic lockout** – disable connection when computer not in use

Firewalls – What to Look For

- **Connection notification** – lets you know when a program attempts to send out from your PC – detects spyware
- **Paranoia level tuning** – pre-configured settings for desired security level
- **Password protected configuration**
- **Configurable rule set** – advanced feature

Personal firewalls – what to do

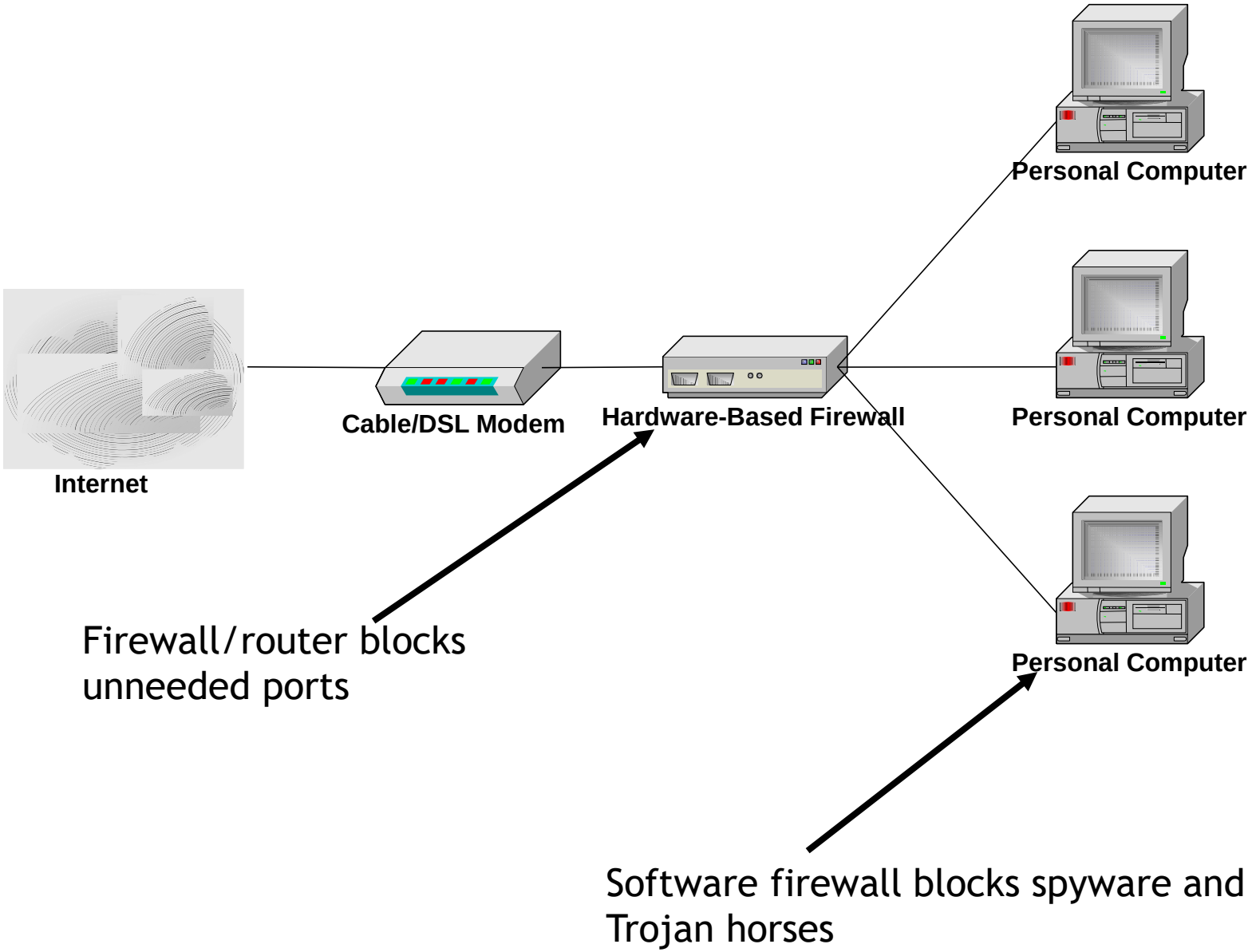
- All home networks connected to the Internet via a broadband connection should have some firewall device installed.
- Install stand-alone hardware firewall
  - Blocks incoming traffic, hides PC
- Install software based firewall
  - Can block suspicious outgoing messages and and alert user
- **Run an online security scan**

Stand-alone Firewalls – How to Set Up

- Change default admin password
- Check for software/firmware updates – software load may have changed since firewall was shipped
- Disable WAN requests – hides existence of PC to unsolicited messages
- Ensure that all unnecessary ports closed
- Restrict or disable remote administration – usually can use direct USB connection for firewall admin

Software Firewalls – How to Set Up

- Log IP address, date/time of infractions
- Drop incoming packets to known insecure services – e.g. NETBIOS if not needed
- Enable stealth mode – no reply to unsolicited packets
- Shut down connection when not in use
- Enable connection notification – to detect spyware


Internet
Cable/DSL Modem
Hardware-Based Firewall
Personal Computer
Personal Computer
Personal Computer
Firewall/router blocks unneeded ports
Software firewall blocks spyware and Trojan horses

Securing Web Browsers

- Browser Plugins – a dozen or more usually
- ActiveX – becoming ubiquitous on IE
- JavaScript – almost impossible to do without
- Java Applets – needed for multimedia
- Cookies – almost universal

Securing Web Browsers – what to do

- Review plugins and disable unneeded ones
- Use built-in Active X security features, take precautions on using it
- Disable cookies unless needed, or allow only session cookies; delete frequently
- Consider use of internet proxy server if very concerned about privacy

Securing PC Configurations – what to do

- **Strong passwords** – most basic requirement
- **Securing file and printer sharing** – only as necessary
- **Updates** - Reducing operating system and application vulnerabilities updates
- **Virus checkers** –essential, configure to run weekly or more often

Securing PC Configurations – what to do

- Protecting yourself from e-mail worms and viruses
- Spyware removal tools
  - Some free tools to remove spyware
  - Some software firewalls can detect spyware
- Encryption software to protect privacy

Home Networking

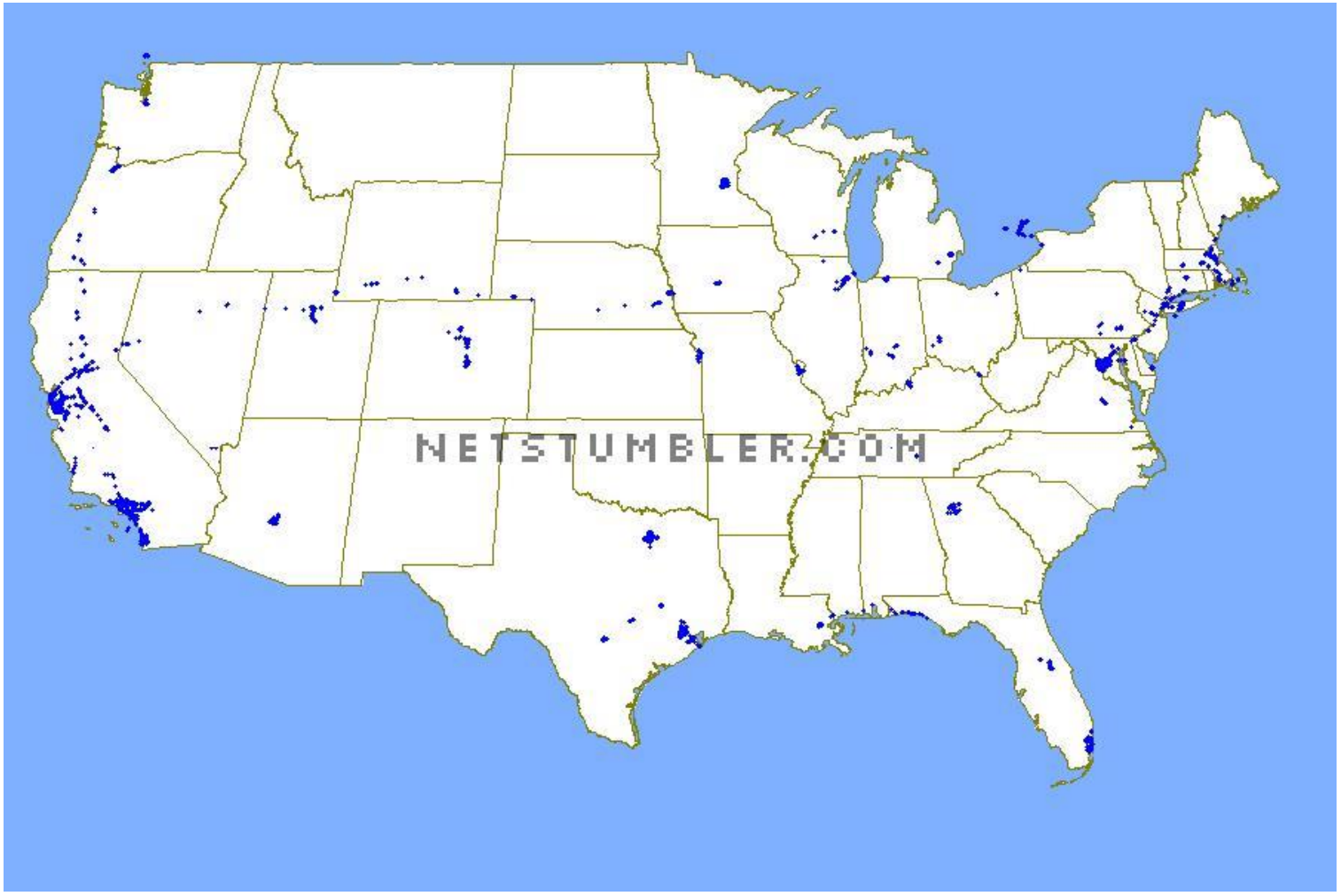
- Ethernet Networking
- Phone-Line Networking (HPNA)
- Power-Line Networking
- Wireless Networking
  - HomeRF
  - 802.11 and 802.11b – WEP intended to provide security equivalent to wired (but doesn't!)

Wireless Networking Security Issues

- Server set ID (SSID) sent unencrypted – attacker can eventually obtain SSID, which enables them to connect to your network
- 802.11b WEP encryption flawed – publicly available software can crack 802.11b with enough packets - home networks reasonably safe, office networks not (theft of service)
- Remote admin (SNMP) with default password
- Denial of service risk inherent in wireless

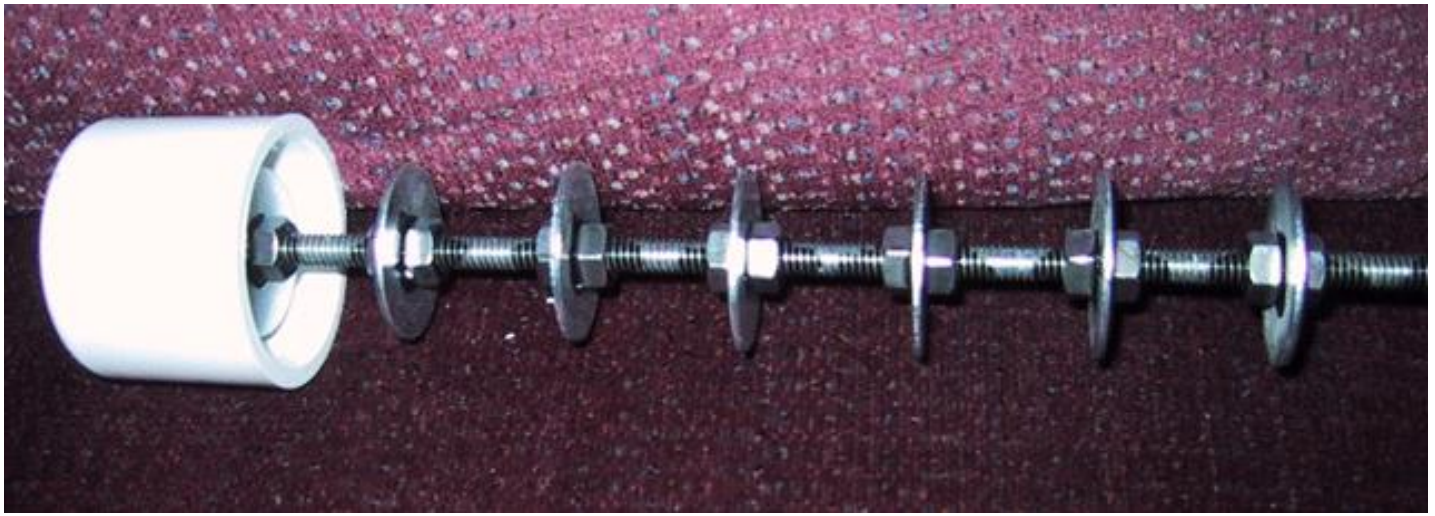
Home Networking Security

- Wired – OK Wireless – not so OK



Wardriving, "drive-by hacking"

- Available on Internet from people with too much time on their hands:
  - Perl scripts to break 802.11b "wired equivalency protocol" (WEP)
  - Plans to build sensitive antennas using parts from Home Depot and Pringles can



"Drive-by hacking" Risks

- **Privacy** – moderate
  - Don't put sensitive information on wireless
- **Theft of service** – more serious
  - Campus or business park – easy for hackers to mask identity – your organization gets blamed for intrusions
  - Home – less concern, but don't ignore

Home Networking – what to do

- Use file and printer sharing only as necessary
- Change default
  - admin passwords and
  - SSIDs
- Use encryption, even if it is not perfect

Virtual Private Networks

- **VPN security** - connectionless integrity, data origin authentication, confidentiality or privacy, traffic analysis protection, access protection
- **VPN modes of operation**
- **VPN protocols**
- **Peer authentication**
- **Policy configuration**
- **VPN operation**

Virtual Private Networks – what to do

- First ensure that needs can't be met with less expensive tools
- Agency system admin responsible for configuring VPN and providing telecommuter with proper software
- Educate users on correct operation

Telecommuting Architectures

- **Voice Communication** – security considerations of different types of phones
- **Electronic Mail** – different ways to handle it based on security requirements
- **Document and Data Exchange**
- **Ways to combine** – to provide voice, email, and document exchange in cost effective ways

Voice Communication

- **Corded phone** – most secure; tapping requires physical connection
- **Cordless** – can be picked up on scanners, baby monitors, etc.; 900 MHz, 2.7 GHz more secure for now
- **Cell phones** – can be picked up with UHF tuner
- **Digital PCS** – more secure for now
- PC based voice communication (Voice over IP) – depends on security of your PC and Internet
- **What to do – get a corded phone for office**

Electronic Mail

- **Remote login** – may use unencrypted passwords (POP3)
- **E-mail forwarding** – user doesn't need to log in to central system at all; OK if email not sensitive
- **Virtual Private Network (VPN)** – great security but expensive and more complex to install/administer
- **What to do**– choose based on cost and what's more important, central system or email contents

Document and Data Exchange

- **Remote connection** – needs good administration
- **FTP and web file transfer** - likewise
- **E-mailing document and data files** – OK if material not sensitive
- **Virtual Private Network (VPN)** – secure but expensive
- **Physical transfer (sneaker net)** – secure but annoying
- **What to do**– choose based on cost and what's more important, central system or document contents

Agency/enterprise Considerations for Telecommuting Security

- **Controlling system access** - strong passwords, one-time password generators, Smartcards, biometrics
- **Protecting internal systems** - restricted access, firewalls and secure gateways, location of resources, proxy servers, encryption
- **Protecting home systems** - **security policy, employee accountability, removable hard drives, data encryption, dedicated use, locked rooms or storage containers, home system availability.**

Agency/enterprise Considerations – what to do

- Establish standard security configuration for telecommuter systems
- Organization should provide pre-configured PC for home user
- Limit use to official duties (but assume this won't always be followed!)

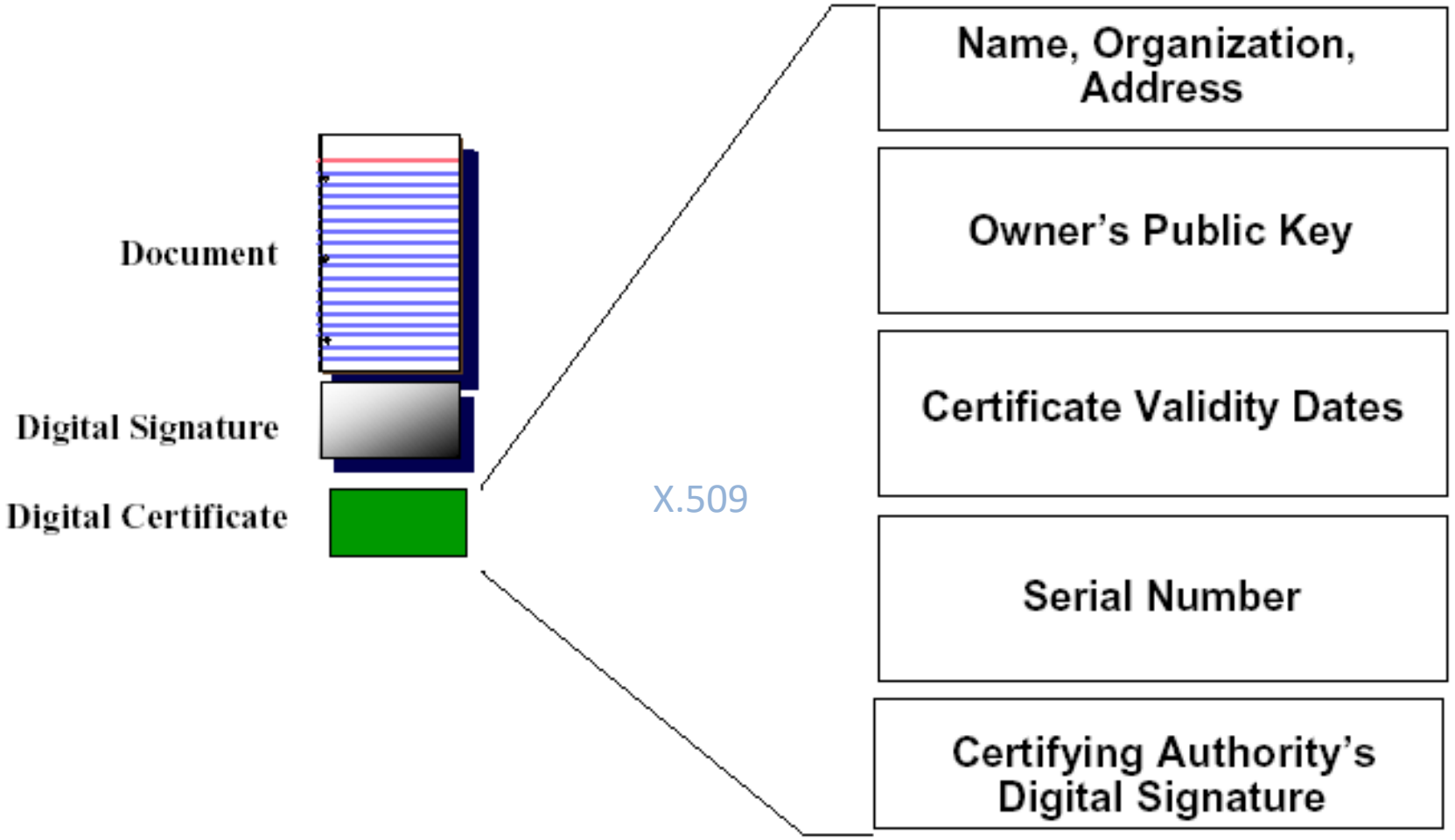
Top 10 User Precautions for Telecommuting

1. Install software firewall
2. Add stand-alone firewall (also)
3. Install anti-virus software
4. Turn off file and printer sharing (unless needed for home network)
5. Update operating system and browser regularly

Top 10 User Precautions for Telecommuting

6. Know how to turn off and delete cookies
7. Use strong passwords
8. Install spyware detection and removal tools
9. Use only amount of security necessary
10. Consider encryption or VPN software if you need it

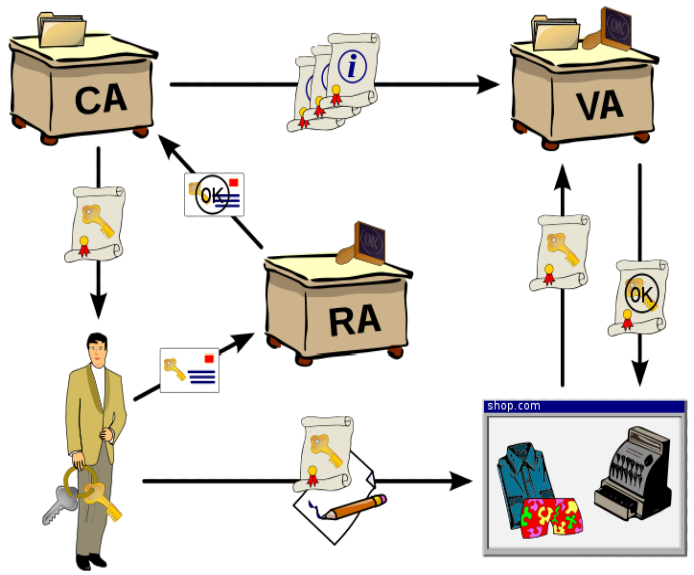
Digital Certificates



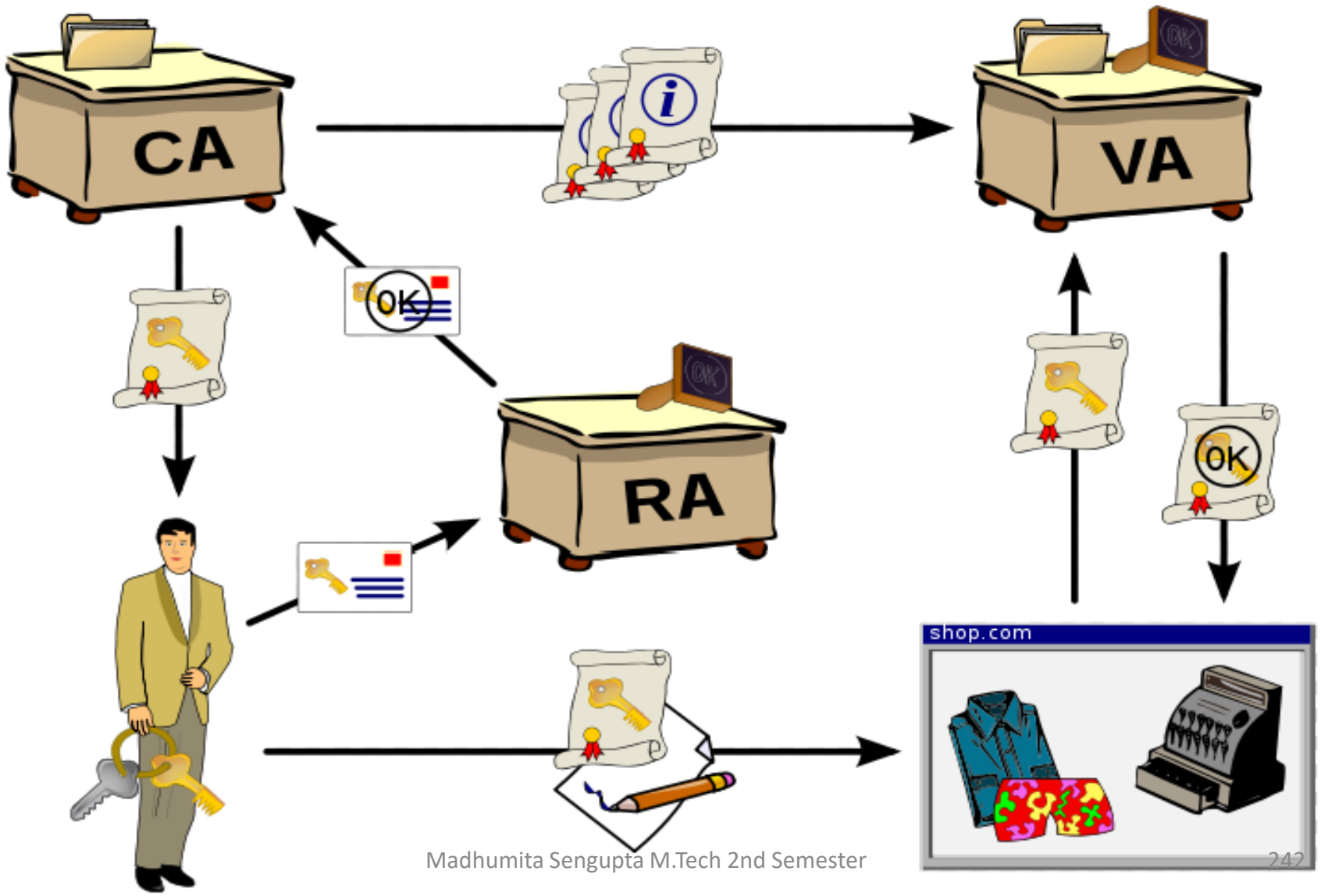
Public Key Infrastructure

The **Public Key Infrastructure** (**PKI**) is the road ahead for almost all cryptography system.

The **PKI** is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates .



Public Key Infrastructure



Public Key Infrastructure

- In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).

- The PKI role that assures this binding is called the Registration Authority (RA).

- PKIX and PKCS are the two popular standards for digital certificates.

Public Key Infrastructure Provides

Privacy and Confidentiality

- Secure Transport
- File Encryption
- Secure e-mail

Authentication

- Network components & end users

Non-repudiation and Data Integrity

- Digital signature
- Trusted time stamp

What Organizations Wants?

- **Certificates that are accepted nationwide for government, commercial, and financial transactions.**
- **A trusted CA with strong internal controls over issuance, distribution, and management.**
- **Policies that are enforceable nationwide.**
- **Liability protection**
- **Reasonable pricing**

Public Key Infrastructure

As we know, X.509 standard defines the digital certificate structure, format and fields. It also specifies the procedure for distributing the public key. In order to extend such standards and make them universal, the Internet Engineering Task Force (IETF) formed the Public Key Infrastructure X.509(PKIX)

STEGANOGRAPHY

STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity (darkness).

SECRET COMMUNICATION

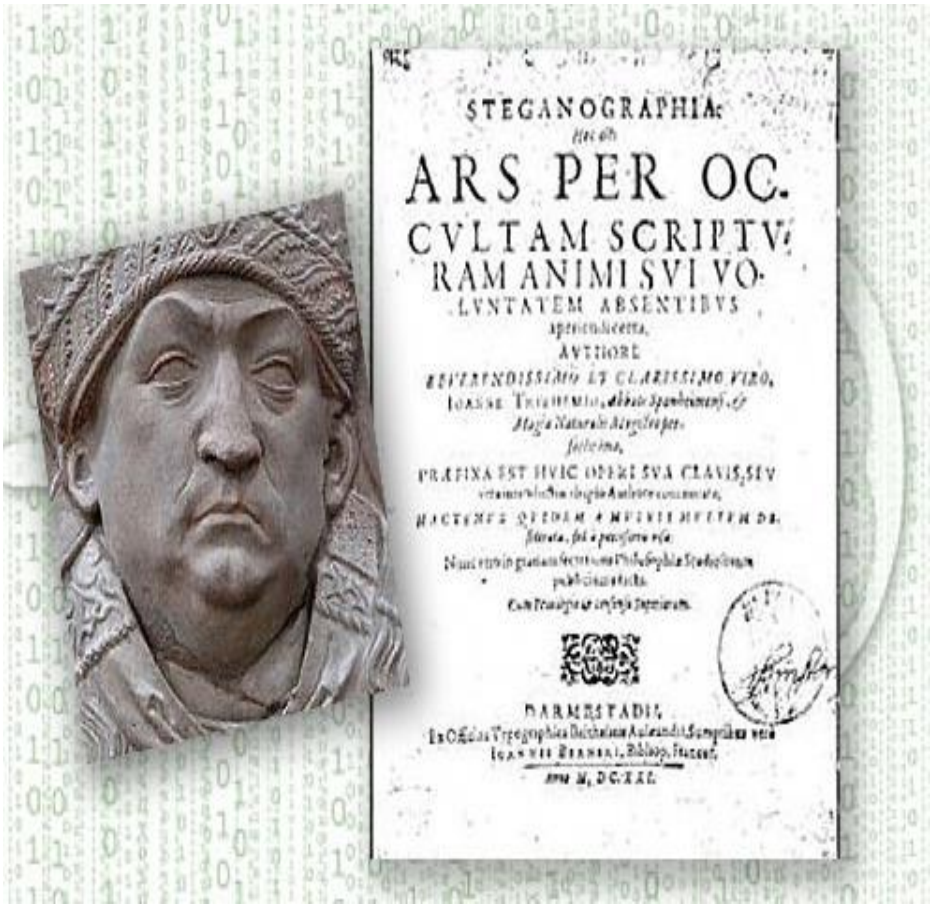
SECRET DATA TRANSFER

IMAGE AUTHENTICATION

1. Great reduction in the risk of information being leaked in transit (IMAGE COMMUNICATION).
2. Owners can protect their work by embedding a watermark.
3. Semitransparent logos are commonly added to TV programs by broadcasting networks.

SECRET COMMUNICATION

Brief history of how the art and science has evolved.



The word steganography came from a 15th century work called Steganographia by a German abbot named Trithemius. On the face of it, the three books were about magic, but they were also contained an encrypted treatise on cryptography – so Steganographia was itself a case of steganography.

SECOND EXAMPLE

An ancient Greek named Histaiaeus was fomenting revolt against the king of Persia and needed to pass along a message secretly. He shaved the head of a slave, tattooed the message on his scalp, then sent him on his way when his hair grew back in. Recipients of the message shaved his head again to read the alert. The Greeks used the same trick shaving and writing on the belly of a rabbit.

THIRD EXAMPLE

Sometime in the 5th century B.C., an exiled Greek named Demaratus wrote a warning that the Persians planned to attack Sparta. He wrote the message on the wooden backing for a wax tablet, then hid it by filling in the wood frame with wax so it looked like a tablet containing no writing at all. The wife of the Spartan king divined that there was a message behind the wax, so they scraped it off and got the warning in time to set up a desperate defence at Thermopylae, incidentally giving modern screenwriters the plot for the movie The 300.

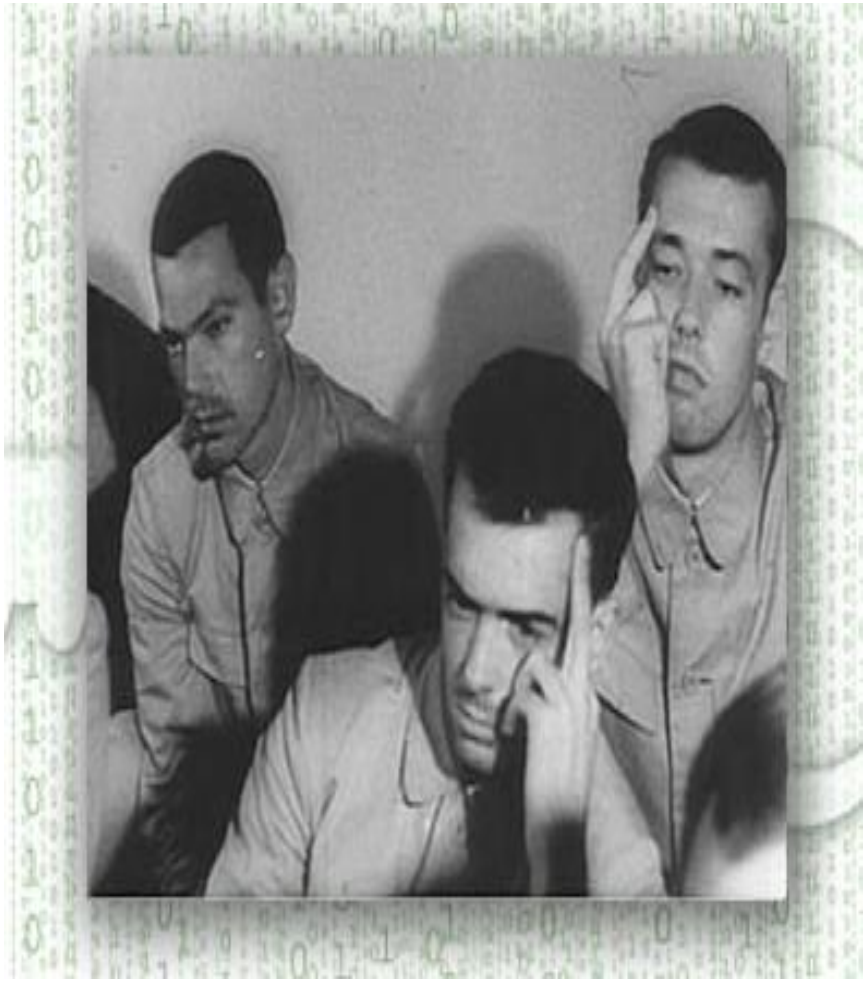
FOURTH EXAMPLE

Encoded messages have been knitted into sweaters and other garments. In this example, the blue dotted lines are Morse Code for, "My girlfriennd knit this." Yes, the sweater has a typo – an extra n in girlfriend - according to the woman who knitted it.

FIFTH EXAMPLE

During World War II, microdots - miniaturized photos that can be hidden in plain sight, then read using magnifiers – were used by spies to carry data out of enemy countries. Here the microdot circled in red piggybacks on a watch face. Blown up, it reveals a message written in German.

Sixth Example



When the USA Pueblo was captured by North Korea in 1968, the crew was forced to pose for propaganda photos to demonstrate they were being well treated. Their finger gestures are a form of steganography that sends a message Americans could decrypt right away, the North Koreans, not so quickly.

Seventh Example

Digital photo steganography uses code fields for unimportant bits as places to hide encoded messages or images. While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. In these pictures, the image of the cat has been embedded in the image of the branches against the sky.

STEGANOGRAPHY

- TRADITIONAL STEGANOGRAPHY.
- MODERN STEGANOGRAPHY.

STEGANOGRAPHIC PROTOCOLS

- Pure Steganography
- Secret Key Steganography
- Public Key Steganography

APPLICATIONS STEGANOGRAPHY

1. Usage in modern printers

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

2. Usage in Legal document

Steganography can be used for digital watermarking, where a message (being simply an identifier) is hidden in an image so that its source can be tracked or verified, copyright protection, Bank draft, cheque and many other.

3. Steganography in audio can be used with mobile phone.

RUMORED USAGE IN TERRORISM

Rumors about terrorists using steganography started first in the daily newspaper USA Today on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July of the same year, the information looked even more precise: "Militants wire Web with links to jihad".

DOCUMENT AUTHENTICATION

We are Indian. We are proud for our co ry. We always like t head with posi and givin to growt We are so muc g in science and Tech logy.

Nabin Ghoshal

Original Document by Sender

Technique to Authenticate

We are Indian. We are proud for our c We always like ead with nega nd giving to growt We are so muc in science and Tech logy.

Nabin Ghoshal

Change Document to Receiver

DOCUMENT AUTHENTICATION

We are Indian. We are proud for our country. We always like to look ahead with positive attitude and giving maximum effort to growth our country. We are so much strong in science and Technology.

Nabin Ghoshal

Tran

We are Indian. We are proud for our country. We always like to look ahead with **positive attitude** and giving **maximum effort** to growth our country. We are so **much strong** in science and Technology.

Nabin Ghoshal

DOCUMENT AUTHENTICATION

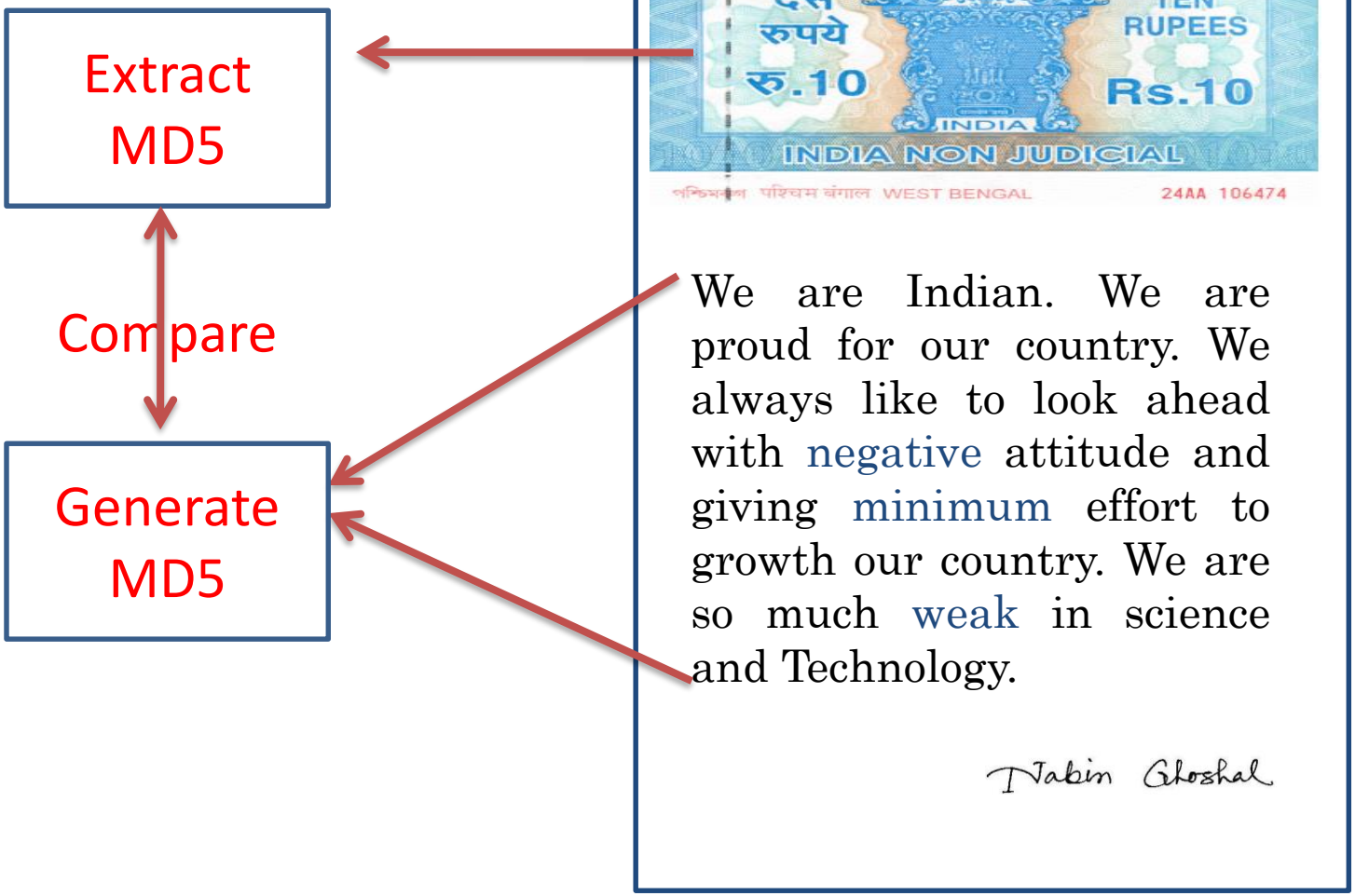


IMAGE AUTHENTICATION

Lena Image

Lena Image

SENDER SIDE OPERATION

IMAGE AUTHENTICATION

Embedded Lena Image

Original Secret Image

COMPARE

Extracted Image

RECEIVER SIDE OPERATION

References

- [1]. Cryptography And Network Security [Atul Kahate]
- [2]. dist-pki-tutorial.html
- [3].http://en.wikipedia.org/wiki/Public_key_infrastructure
- [4]. http://www.pki-page.org/
- [5]. http://www.isg.rhul.ac.uk/cjm/pkis.pdf
- [6]. http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/standards-specifications.htm
- [7].http://www.comms.scitech.susx.ac.uk/fft/crypto/understanding_pki. pdf

THANK YOU