African Virtual University

Applied Computer Science: CSI 5101

MOBILE AND WIRELESS COMPUTING

Dancan K Kibui

Foreword

The African Virtual University (AVU) is proud to participate in increasing access to education in African countries through the production of quality learning materials. We are also proud to contribute to global knowledge as our Open Educational Resources are mostly accessed from outside the African continent.

This module was developed as part of a diploma and degree program in Applied Computer Science, in collaboration with 18 African partner institutions from 16 countries. A total of 156 modules were developed or translated to ensure availability in English, French and Portuguese. These modules have also been made available as open education resources (OER) on oer.avu.org.

On behalf of the African Virtual University and our patron, our partner institutions, the African Development Bank, I invite you to use this module in your institution, for your own education, to share it as widely as possible and to participate actively in the AVU communities of practice of your interest. We are committed to be on the frontline of developing and sharing Open Educational Resources.

The African Virtual University (AVU) is a Pan African Intergovernmental Organization established by charter with the mandate of significantly increasing access to quality higher education and training through the innovative use of information communication technologies. A Charter, establishing the AVU as an Intergovernmental Organization, has been signed so far by nineteen (19) African Governments - Kenya, Senegal, Mauritania, Mali, Cote d'Ivoire, Tanzania, Mozambique, Democratic Republic of Congo, Benin, Ghana, Republic of Guinea, Burkina Faso, Niger, South Sudan, Sudan, The Gambia, Guinea-Bissau, Ethiopia and Cape Verde.

The following institutions participated in the Applied Computer Science Program: (1) Université d'Abomey Calavi in Benin; (2) Université de Ougagadougou in Burkina Faso; (3) Université Lumière de Bujumbura in Burundi; (4) Université de Douala in Cameroon; (5) Université de Nouakchott in Mauritania; (6) Université Gaston Berger in Senegal; (7) Université des Sciences, des Techniques et Technologies de Bamako in Mali (8) Ghana Institute of Management and Public Administration; (9) Kwame Nkrumah University of Science and Technology in Ghana; (10) Kenyatta University in Kenya; (11) Egerton University in Kenya; (12) Addis Ababa University in Ethiopia (13) University of Rwanda; (14) University of Dar es Salaam in Tanzania; (15) Universite Abdou Moumouni de Niamey in Niger; (16) Université Cheikh Anta Diop in Senegal; (17) Universidade Pedagógica in Mozambique; and (18) The University of the Gambia in The Gambia.

Bakary Diallo

The Rector

African Virtual University

Production Credits

Author

Dancan Kibui

Peer Reviewer

Florence Tushabe

AVU - Academic Coordination

Dr. Marilena Cabral

Overall Coordinator Applied Computer Science Program

Prof Tim Mwololo Waema

Module Coordinator

Victor Odumuyiwa

Instructional Designers

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Media Team

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Copyright Notice

Supported By

AVU Multinational Project II funded by the African Development Bank.

Table of Contents

Course Overview

Welcome to Mobile and wireless computing

This course introduces the concepts of wireless / mobile communication using cellular environment. To make the students to know about the various modulation techniques, propagation methods, coding and multi access techniques used in the mobile communication. Various wireless network systems and standards are to be introduced.

Prerequisites

1. Advanced operating systems

2. Data communications and computer networks

Materials

The materials required to complete this course are:

- Spectrum analyzer
- Wireless multi antenna scanner
- RF signal generator

Course Goals

Upon completion of this course the learner should be able to :

- Identify and explain the basic concept of evolution of wireless networks;
- Describe by comparing and contrasting multiple division techniques, mobile communication systems, and existing wireless networks;
- Analyze the security measures in a mobile and wireless computing ..

Units

Unit 1: INTRODUCTION TO MOBILE AND WIRELESS COMPUTING

Evolution Of Mobile Radio Communications- Introduction-

Frequency Reuse- Channel; Assignment Strategies- Handoff Strategies- Interference

And System Capacity- Trunking And Grade Of Service- Improving Capacity In Cellular

Systems.

Unit 2: MULTIPLE ACCESS TECHNIQUES AND WIRELESS NETWORKING

Introduction- FDMA-TDMA- Spread Spectrum - Multiple Access: Space Division Multiple Access- Packet Radio- Introduction To Wireless Networks- Differences Between Wireless And Fixed Telephone Networks- Development Of Wireless Networks- Traffic Routing In Wireless Networks- Integrated Services Digital Network (ISDN)-Protocols For Network Access

Unit 3: WIRELESS SYSTEMS AND STANDARDS

Global System for Mobile - CDMA Digital Cellular Standard (IS-95) - CT2 Standard for Cordless Telephones- Digital European Cordless Telephones (DECT)

Unit 4: MOBILE AND WIRELESS SECURITY

Security Primer- Creating A Secure Environment-Threads- Technologies- Other Security Measures WAP Security Measures- Smart Client Security- Overview of Smart Client

Assessment

Formative assessments, used to check learner progress, are included in each unit. Summative assessments, such as final tests and assignments, are provided at the end of each module and cover knowledge and skills from the entire module. Summative assessments are administered at the discretion of the institution offering the course. The suggested assessment plan is as follows:

1	Introduction	[Enter assessment grading value/weight]
2	Multiple access techniques and wireless networking	[Enter assessment grading value/weight]
3	Wireless systems and standards	[Enter assessment grading value/weight]
4	Mobile and wireless security	

Schedule

Unit	Activities	Estimated time
1. Introduction	At the end of the topic the learner should be able to identify The cellular concept, basic building blocks of cellular systems, handoffs, power control, traffic engineering	[Enter text here]
2. Multiple access techniques and wireless networking	At the end of the topic the learner should be able : • To investigate common digital communication techniques in the time and frequency domains ƒ • To characterize digital communication performance by performing eye pattern and constellation measurements ƒ • To gain experience using a Vector Signal Analyzer ƒ • To demonstrate the use of pulse shaping Frequency division multiple access, time division multiple access, code division multiple access and random access techniques	[Enter text here]

3. Wireless networking	At the end of the topic the learner should be able : • Identify the basic concept of wireless networks; • Analyse traffic theories, mobile radio propagation, channel coding, and cellular concepts; • Compare and contrast multiple division techniques, mobile communication systems, and existing wireless networks; • Classify network protocols, ad hoc and sensor networks, wireless MANs, LANs and PANs; • Apply wireless ID technologies, in particular RFID work.	[Enter text here]
4. Mobile and wireless security	• At the end of the topic the learner should be able : • Describe the operation of cryptographic algorithms and protocols underlying network security applications in mobile systems. • Develop the ability to design and analyze authentication protocols. • Discuss the issue of key management and routing in mobile wireless networks. • Describe the current Web technologies security mechanisms, their attacks and countermeasures. • Develop sufficient knowledge to protect Web applications.	[Enter text here]

Readings and Other Resources

The readings and other resources in this course are:

Unit 1

Introduction to mobile and wireless computing

Required readings and other resources:

- Wireless Communication and Networks - William Stallings PHI , New Delhi 1st edition.
- Wireless and Mobile Networks Concepts and protocols - Dr.Sunilkumar S.Manvi & Mahabaleshwar S.Kakkasageri - Wiley Publisher First Edition
- Mobile Computing for Beginners - Raksha Shende Shroff Publishers and Distributors -First Edition -Feb 2012

Unit 2

Required readings and other resources:

- Arad, M. A. and A. Leon-Garcia . 1998. "A generalized processor sharing approach to time scheduling in hybrid CDMA/TDMA," Proc. IEEE Infocom'98, San Francisco, CA, March, 1164–1171
- Gibson, J. D. ed. 1996. The Mobile Communication Handbook, Boca Raton, FL, CRC Press/IEEE Press

Optional readings and other resources:

- R.J. Pickholtz, L.B. Milstein, and D.L. Shilling,"Spread Spectrum for Mobile Communication," IEEE Trans. on Vehicular Technology 40 R.J. Pickholtz, L.B. Milstein, and D.L. Shilling,"Spread Spectrum for Mobile Communication," IEEE Trans. on Vehicular Technology 40

Unit 3

Required readings and other resources:

- Ganz, A., Ganz, Z., & Wongthavarawat, K. (2003). Multimedia Wireless Networks: Technologies, Standards and QoS. Pearson Education.
- BOJKOVIĆ, Z., MILOVANOVIĆ, D., & SAMČOVIĆ, A. (2002). Multimedia Communication Systems: Techniques, Standards, Networks.
- Optional readings and other resources:
- Garg, V. K., & Rappaport, T. S. (2001). Wireless network evolution: 2G to 3G. Prentice Hall PTR.

Unit 4

Required readings and other resources:

- "Security and Cooperation in Wireless Networks" by Levente Buttyan and Jean-Pierre Hubaux, 2007
- "Implementing 802.1X Security Solutions for Wired and Wireless Networks", Jim Geier, 2008

Optional readings and other resources:

- W. Stallings and L. Brown, "Computer Security: Principles and Practice", Prentice Hall, 1st Ed., 2008, ISBN 0-13-600424-5.
- "Security In Wireless LANS And MANS," Thomas Hardjono, Lakshminath R. Dondeti , 2005

Unit 0. Pre-Assessment:Getting ready for this module

Unit Introduction

This unit is an introductory survey of artificial intelligence. The course will cover the history, theory, and computational methods of artificial intelligence. Basic concepts include representation of knowledge and computational methods for reasoning. The successful student will finish the course with specific modeling and analytical skills (e.g., search, logic, probability), knowledge of many of the most important knowledge representation, reasoning, and machine learning schemes, and a general understanding of AI principles and practice. The course will serve to prepare the student for further study of AI, as well as to inform any work involving the design of computer programs for substantial application domains.

Unit Objectives

Upon completion of this unit you should be able to:Identify the major classical and modern AI paradigms, and explain how they relate to each other

Analyze the structure of a given problem such that they can choose an appropriate paradigm in which to frame that problem

Implement a wide variety of both classical and modern AI algorithms.

.

Key Terms

Analog modulation: (traditional) method of transmitting voice signals where the radio carrier wave is directly based on electrical voltages or currents caused by a user speaking into the microphone, or similar transmission of a signal which takes values from a continuous range of values as opposed to from a finite alphabet of values

Base station: a land station at a fixed location supporting radio access by mobile users to a fixed communication infrastructure.

Bit Error Rate: BER.

Burst: the physical (electric or electromagnetic) contents of a time slot

Capture: successful transmission of a data packet despite interference from other terminals transmitting a conflicting signal. Occurs due to differences in received signal power, or signal separation properties of the receiver or the modulation method.

Code Division Multiple Access:CDMA. Multiple access method based on spread spectrum in which different users transmit on (approximately) the same carrier frequency, but use different spreading codes.

Cell: the area covered by radio signals from a base station, and in which a mobile station can successfully transmit to a base station

Cellular network: Network in which frequencies are reused in a regular pattern, usually with basic area elements of hexagonal shape

Cell splitting: A method of increasing capacity by reducing the size of the cell.

Circuit-switching: the allocation of network resources (link capacity, switches) for the entire duration of a communication session.

Cluster size:number of different channels needed in a particular frequency reuse plan. Related to reuse distance.

Coding: intentional replacement of a set of symbols by another set of symbols. Applications are detection or correction of errors, spectral shaping of the transmit signal, or confidentiality.

Collision: conflicting simultaneous transmission by multiple terminals in a random access network.

Coverage area: part of the area to which a transmitter gives satisfactory

service

Decibel: a ratio, expressed as ten times the base-10 logarithm of the ratio of two power levels. This is equivalent to 20 times the base-10 logarithm of the ratio of two voltage, field or current levels.

Digital Enhanced Cordless Telephone: DECT.

Previously: Digital European Cordless Telephone. Operates in 1800 MHz band.

Delay spread: parameter describing the frequency dispersion of a multipath channel. 1) **total delay spread:** time interval during which delayed reflected waves arrive. 2) rms **delay spread:** weighted value of interarrival times of reflected waves

digital modulation:A method of transmitting a signal over a radio carrier using symbols of an alphabet of finite size, such as the computer's binary 0s and 1s.

dispersion: variations in the channel transfer amplitude. Frequency dispersion: differences in channels response at different frequencies. Time dispersion: time variations of the channel response

diversity: technique of receiving a radio signal through multiple channels, to improve reliability.

doppler spread: (one half times the) width of the spectrum of a received signal when a sinusoidal wave is transmitted over a time dispersive channel

downlink: Originally: A radio link from a satellite to a receiving site on earth or in an aircraft. Now also used for the (forward) link from base station to portable terminal.

Direct Sequence: DS. form of spread-spectrum in which the user signal is multiplied by a fast (spectrally broad) code sequence to increase the transmission bandwidth.

Digital Short Range Radio: DSRR. system for short range communication. For in stance between a car and a roadside base station or gantry.

duplex: Method of operating a network in which transmission is possible simultaneously in both directions of a telecommunications channel.

equalization: signal processing (filtering) intended to undue channel dispersion. Mostly a compromise is made between combating channel dispersion and avoiding undesirable noise enhancements

European Telecommunications Standards Institute:ETSI.

European organization responsible for establishing common industry-wide telecommunication standards.

fading: Time variations of the signal strength received over a radio link. Fading occurs when the several reflected waves (destructively or constructively) interfere with each other.

Federal Communications Commission: FCC. U.S.

Frequency Division Multiple Access: FDMA.

Multiple access method in which different users transmit at different carrier frequencies.

flat fading: frequency-nonselective fading. Form of fading that does not cause intersymbol interference.

frequency modulation: FM. analog modulation method, exploiting variations in the instantaneous carrier frequency

Frequency Shift Keying: FSK. digital frequency modulation method

free space loss: FSL. power loss due to the spreading of energy over the surface of a sphere as the signal travels away from the transmit source.

Geosynchronous Earth Orbit: GEO.

satellite communication system.

GMSK: Digital phase (or frequency) modulation method, for instance used in GSM

GSM: previously Groupe de travail Speciale pour les services Mobiles. Widely used digital cellular phone standard, initiated in Europe.

handover: action of changing the handling the operation and control of a radio link from one base station to another as the user moves from one cell to another.

half duplex: communications system that supports conversation in two directions but not simultaneously by sharing a communication path between the two directions

Hertz: unit of measuring the frequency of a signal.

hidden terminal: terminal in a CSMA network actively transmitting data, but which is not noticed by another terminal with data ready for transmission.

Intelligent Network: IN. A secondary network used to create and deliver advanced services to subscribers to public telephone networks (fixed or mobile)

in-phase component: component of a signal that has the same phase as a reference sinusoidal signal.

interference: signals from other emitters than from transmitter sending the wanted signal. Interference differs from noise in that interference often contains similar waveforms as the wanted signal

interleaving: intentional resequencing (shuffling) of the bits in a signal according to a predefined method known by both transmitter and receiver, to avoid burst errors.

Unit Assessment

Check your understanding!

1. Distinguish between 1G and 2G cellular networks.
2. Define a cell.
3. What is frequency reuse?
4. What are the various types of wireless network topologies?

5. Mention the various multiple access schemes used in wireless communication.

6. What is co-channel interference?

7. Mention the different types of cells.

8. What is a picocell?

9. What is cellular topology?

10. What is a cluster?

11. What are the technical issues in planning of a cellular network?

12. What is cell splitting?

13. What are the different types of Handover?

14. What are the applications of a satellite system?

15. What are the basic units of a Cellular system?

16. What are the limitations of conventional mobile telephone system?

17. What is SIM?

18. What are main subsystems of GSM architecture?

19. What are the types of services in GSM?

20. Mention the function of the base station.

Instructions

Attempt all the questions

Grading Scheme

Each question carries 2 marks

Feedback

1. First generation cellular systems introduced in early 1980's were based on analog FM technology and designed to carry narrowband circuit switched voice services. Second generation cellular systems introduced in early 1990's use digital modulation and offers more spectral efficiency and voice quality.

2. In mobile communication, the coverage area is divided into smaller areas which are each served by it's own base station. These smaller areas are called cells.

3. Spatially reusing the available spectrum so that the same spectrum can support multiple users separated by a distance is called frequency reuse.

4. Infrastructure network topology and ad hoc topology.

5. Frequency Division Multiplexing Access, Time Division Multiplexing Access and Code Division Multiplexing Access

6. Interference between signals from co channels are termed as co channel interference

7. Femtocells, picocells, micro cells, macrocells and mega cells.

8. Small cells inside a building that support local indoor networks such as wireless LANs. Size of these cells are in the range of few tens of meters.

9. Cellular topology refers to infrastructure topology employing frequency reuse concept.

Selection of frequency reuse pattern for different radio transmission techniques

. Physical deployment and radio coverage modeling

. Plans to account for the growth of the network

Analysis of the relationship between the capacity, cell size and the cost of

infrastructure

10. This is the process of subdividing a congested cell into smaller cells, each with it's own base station and a corresponding reduction in antenna height and transmitter power. Cell splitting increases the capacity of a cellular system since it increases the number of times that channels are reused.

11. Intra-satellite hand over • Inter-satellite hand over • Gateway hand over • Inter-system handover

12. Weather forecasting. • Radio and TV broadcast satellites. • Military services. • Navigation.

13. Mobile stations • Base stations • Mobile Switching Center (MSC) or Mobile Telephone Switching Office (MTSO).

14. Limited service capability • Poor service performance • Inefficient frequency spectrum utilization

15. SIM, which is memory device that store information such as the subscriber identity number, the network and countries where the subscriber is entitled to service, private key, and other user specified information.

16. i) Base station subsystem (BSS) ii) Network switching subsystem (NSS) iii) Operation support subsystem (OSS)

17. Tele services and Data services

18. The base station serves as a bridge between all mobile users in the cell and connects the simultaneous mobile calls via telephone lines or microwave links to the mobile switching center(MSC)

Unit Readings and Other Resources

The readings in this unit are to be found at the course-level section "Readings and Other Resources".

Unit 1. Introduction to Mobile and wireless Computing

Unit Introduction

This unit allows the student to gain knowledge about the evolution of radio communication systems.and to have a good understanding of radio waves. We will study the propagation of radio waves, in particular and some of the problems related to radio interference.

Unit Objectives

At the end of this unit the learner should be able to:

- Describe the evolution of radio communications;
- Illustrate allocation and radio frequency reuse strategies
- Describe the different strategies to improve the capacity of cellular systems

Key Terms

ETSI. (European Telecommunications Standards Institute), that is the European telecommunications standards Institute, is the European standardization body in the field of telecommunications

SRD (Standard Radar Definitions) the international organization of frequency control.

CDMA (Code Division Multiplexing Access) spread spectrum (division by code)

Network AMPS (Advanced Mobile Phone Service) in the USA (Chicago, aT & T, 1979); 1 global system subscribers until 1997

Network NMT (Nordic Mobile Telephony) Sweden (Ericsson, 1981)

Network TACS (Total Access Coverage System adapted from AMPS to 900MHz) in UK (Vodafone, former Racal Telecoms 1985)

RADIOCOM Network 2000 (450MHz) in France (France Telecom, 1985)

DECT (Digital European Cordless Telecommunications) - European standard for digital voice radio point to point between a phone or a light portable terminal and a station based. The DECT standard provides for the transfer = inter cell roaming)1995).

IS-95: US second-generation system:

PDC Japanese second generation system

Personal PHS: Handset System (replaces the pager; no cell; Low tariff at high speed (64 kbit / s) limited

CT2mobility. digital radio standard wireless. CT2 defines small handheld devices for calling communicating through intermediate terminals located a few hundred meters, but not receive

GSM. GSM: TDMA-based, standard originated in Europe but used worldwide

GSM / IS-54 mobile phones 2nd generation

PCS. (Personal Communication system)

CDMA 2000 standard to supplant American CDMA-One system. allows data rates up to 140 kbits / s

UMB. (Ultra Mobile Broadband) proposed by Qualcomm to improve the CDMA2000 but was abandoned in November 2008 in favor of LTE

GPRS. packet switching technique on GSM. Mobile telecommunication network to packet switching. GSM Evolution for transmitting packet multimedia data, at high speeds, in the context of existing radio infrastructures

MS:.(Mobile Station) A GPRS mobile station (MS, can operate in one of the following classes

EDGE.: (Enhanced Data rate for GSM evolution) is an evolution of a GPRS standard and it has been available since 2003 and allows data rates up to 230 kbit / s

UMTS.(Universal Mobile Telecommunications System) is the evolution of GSM to provide 3G services.

HSPA (High Speed Packet Access) is a generic term adopted by the UMTS Forum to name the improvement of UMTS radio interface. HSPA mean enhancements to both the downward flow (HSDPA) and upflow (HSUPA). As part of the evolution of GSM to 3G, HSPA enables faster data transfer, to enhance spectral efficiency and increase the capacity of operators of systems. Regarding users, HSPA provides access to a world of mobile high débitmultimédia

HSDPA. (High-Speed Downlink Packet Access) Evolution of UMTS that advances the receipt flows (in the direction towards the network terminal) to 2 Mbit / second (and, if one believes handset providers; 3 Mbps and up to 14 Mbit / s

LTE. (Long Term evolution) is the evolution dde HSDPA Mobile.

IMSI (International Subscriber Identity) is a unique number that allows a mobile network GSM, UMTS or LTE to identify a user. This number is stored in the SIM card (USIM in UMTS and LTE) and is not known to the user . to achieve this, the operator assigns a MSISDN which is the version with international prefix of what is commonly called a "mobile phone number"card.

SIM (Subscriber Identity Module) is a chip containing a . microcontroller and memory and is used in mobile phones to store information specific to a subscriber of a mobile network, especially for GSM, UMTS and LTE

MSISDN. (msisdn) is number "public knowledge" of the GSM or UMTS user as opposed to the IMSI number. It is this identifier, commonly called telephone number, which will be made to reach the subscriber. Only the HLR (Home Location Register) knows the correspondence between the MSISDN and IMSI number in the SIM card of the subscriber

IP. Internet Protocol

VSAT: Very Small Aperture Terminal

USAT: Ultra Small Aperture Terminal

FAMA: Fixed-assignment multiple Access

RA: Random Access

AP: Packet Reservation

DAMA: Demand Assignment Multiple Access

LAN: Local Area Network

Metropolitan MAN:Area Network

WAN: Wide Area Network

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WWAN: Wireless Wide Area Network

Activities of learning

Activity 1.1 - Background and evolution of radio communications

1. **Introduction**

Wireless communication is the transfer of information over a distance without the use of an electrical conductor or wire. The distances can be very short (in the image of a television remote control) or very long (approximately 1000 km or thousands of km for wireless communication). However, the term "wireless" is used in both situations. Wireless communications are considered a branch of telecommunications.The term “**wireless”** is used to describe telecommunications in which electromagnetic waves are used to carry the signal over part or end to end communication. As an example we can mention:

- Mobile phones or pagers (beepers): their purpose is to provide connectivity for portable and mobile applications, both personal and professional
- GPS (Global Positioning System): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to determine their location anywhere on earth.

Mobile history

communications world “telecommunication” comes from the Greek prefix ‘tele’ meaning “far” and the Latin “ communicare “which means” to share “. In ancient times, the communication was appeared by modulating the light ON and OFF. In the years 150 BC, the Greeks had to use smoke to communicate. This shows that humans had all the time needed to communicate without the use of physical media. The timeline below shows the turning of wireless communication:

- 1794 Shape Claude invented the optical telegraph for wireless long distance
- 1834-1874, Johann Philipp Reis discovered the principles of the telephony,
- 1835 Morse code was invented by Samuel Morse telegraphy
- 1886 Heinrich Hertz discovered the electromagnetic waves in the
- Air,1906, Robert von Lieben invented the vacuum tube
- 1937, Guglielmo Marconi invented wireless telegraphy
- 1958 establishment of the first network in Germany “A.Netz” which was analog with a 160 MHz carrier frequency.
- 1972, B.Netz network will always follow in Germany using the same 160 MHz frequency. Here the current position of the mobile receiver must be known.
- 1981, the mobile telephone service Nordic (NMT) was developed with the 450 MHz band as carrier
- 1982. Inmarsat is a satellite was launched
- In 1984, The Cordless Phone (CT1) to following its predecessor, the 1980 CT0, was launched. This is the birth of the first generation
- 1987 networks,CT2 has been developed and it uses the spectrum at 864 MHz and offers a data channel with a rate of 32 Kbit / s
- 1991 ETSI has adopted the European standard Digital Cordless Telephone (DECT) for wireless digital telephone with 1880-1900 MHz spectrum. At that time the access technology Code Division Multiple Access (CDMA) has also been improved
- In 1992, the Global System for Mobile communication (GSM) has been standardized

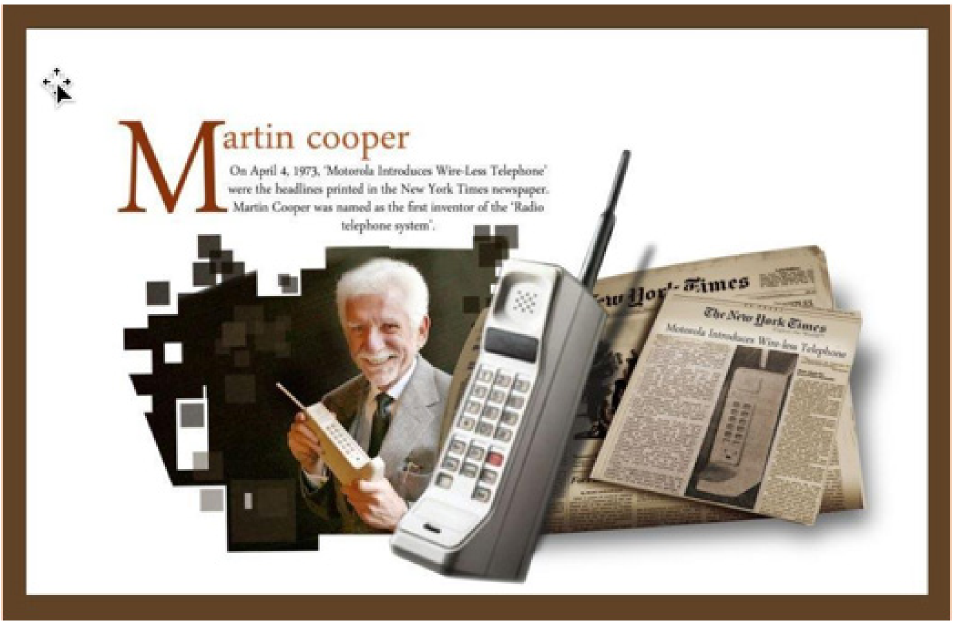
- 1994, GSM 1800 networks in Europe also known as DCS 1800 (Digital Cellular system) have started with better quality
- 1996 HiperLAN (High Performance Radio LAN) is standardized by ETSI
- 1998 mobile systems of universal telecommunications (UMTS) were developed by European in 1999, Bluetooth was standardized
- In 2000, General Packet radio Service (GPRS) a was developed.
- 2001, IMT-2000 (International Mobile Telecommunications for the year 2000) is the acronym chosen by the ITU to designate five radio access technologies for cellular systems of the third generation 2007 the 4G based on an "All-IP" network core has emerged.

The mobile phone?

it is called mobile phone, or mobile phone, or cell phone and it has revolutionized our quotidien.Il allowed us to call in the first version aujourdui but it allows us to call to send and receive data.

the mobile phone is born from multiple technologies, some of which were already known in the late 1940s However, authorship is attributed to Martin Cooper and Joel Engel who were engineers in the laboratories of the firm Motorola. The first call telephone was conducted in April 1973 by themselves.

In 1983, Motorola has been launched in the United States the first real mobile phone called Motorola DynaTAC 8000X which measured 25 cm (not including the antenna) and a weight of 783 grams . If these dimensions seem excessive to you today, it was good at the time of the smallest cell phone ever created A.1.1.1.



Martin cooper

On April 4, 1973, 'Motorola Introduces Wire-Less Telephone' were the headlines printed in the New York Times newspaper. Martin Cooper was named as the first inventor of the 'Radio telephone system'.

Figure The Motorola DynaTAC 8000X said BRICK PHONE

Source: http://simplyknowledge.com /uploads/script/martincooper/Martin-Cooper-here-bg.jpg

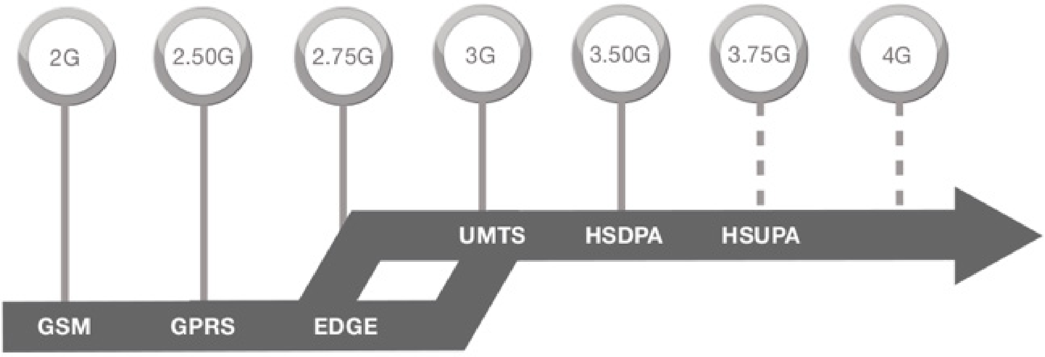
The boom in mobile telephony has arrived with the second generation (2G) network around the year 1990. These mobile phones using the GSM (Global System for Mobile communications). Currently, we are seeing the third generation phones advent (3G) and even fourth-generation (4G). There is also an interoperable mobile communications sytsèmes. The phones integrate many innovations that send sounds, videos, to video conferencing, watch TV, surf the Internet, electronic door currency, etc. Users can access different services anywhere, anytime. We are in the era of ubiquity. This is possible thanks to the interoperability.

Network types

- Wireless Personal Area Networks (WPAN)
- WPAN is used for the short distances between nearby equipment. We can classify them into the following groups:
- technologies:.Bluetooth (IEEE 802.15.1) launched by Ericsson in 1994, offering a maximum throughput of 1 Mbps to a maximum range of about thirty meters Frequency range 2.4 to 2.483 GHz
- HomeRF (Home Radio Frequency), This was launched and proposed a theoretical speed of 10 Mbps with a range of about 50 to 100 meters without an amplifier. It was abandoned 2003. The
- in ZigBee (IEEE 802.15.4) it provided wireless connections at very low cost and with very low energy consumption. This technology was adapted to be directly integrated into small electronic devices (appliances, stereo, toys, sensors, etc.).
- The infrared links were used to create connections without dependence of a few few meters with speeds up up to a few megabits per second. This technology is widely used for home automation(WLAN).
- Wireless Local Area Networks
- Its main application is in public places (eg universities, airports, companies, private). The main problem with this type of network is often an operating time of 2.4 GHz (802.11b) it is much prone to interference from wireless phones. This technologies appear in different subgroups as listed below:
- WiFi (or IEEE 802.11), supported by the WECA alliance (Wireless Ethernet Compatibility Alliance) offers speeds up to 200 Mbps over a distance of about 2 metres .Hiper LAN2 (High Performance Radio LAN 2) is European standard developed by ETSI (European Telecommunications Standards Institute), which provides a theoretical speed of 54 Mbit / s over an area of one hundred meters in the frequency range between 5150 and 5300 MHz
- DECT (Digital Enhanced Cordless Telecommunications) is a standard that does not depend on local area networks
- Wireless Metropolitan Area Networks
- WMAN are used to serve big cities and are also referred by the name name Local (WLL).WMAN are based on IEEE 802.16.
- Phase 3 WiMAX offers speeds of 1Gbit / s. The version of WiMax can be seen as alternative to ADSL for rural areas.
- Wide wireless area networks(WWAN)

- WANs represent the traditional technologies of voice and data transport.
- There are other technologies that are related to WANs:
- GSM (Global System for Mobile communication : originally the GSM standard only used a radio frequency band around 900 MHz. It was extended to two other bands around 1800MHZ and 1900MHZ under the DCS names 1800 and DCS 1900 (standard used mainly in the United States).
- GPRS (General Packet Radio is a Service).This is a switching technique on the frequency bands 900 MHz and 1800 MHz. The standard, which is based on the fact that only the useful packets are transmitted, provides opportunities such as sharing resources among multiple users through an appropriate bandwidth allocation.
- UMTS (Universal Mobile Telecommunication System) uses a neighboring frequency range of 2 GHz. The UMTS coverage is divided into a large variable-sized cells. Each cell has a function of population density to be used and the speed of mobility.
- EDGE (Enhanced Data Rate for GSM Evolution).This is is an intermediate technology between GSM and UMTS available since 2003. It provides quick access to the internet at a speed of 200 Kbit / s for stationary users.
- HSPA (high speed Packet access) provides access to a world of mobile high-speed multimedia services. It means improvements in both downflow (HSDPA) and upflow (HSUPA). It enables faster data transfer, to enhance spectral efficiency and increase the capacity of operators of systems.
- 4G is based on an IP core, It is a the convergence of multiple networks, and does not cause technological break with the 3G (UMTS). It provides high-speed data access, enabling uninterrupted service transmission between multiple radio access points.

Figure A.1.1.2 below shows the evolution of WAN technologies



Source: Felix Singo, OS12 Module

The following satellite launch can also be considered in wireless networks:

- The first satellite was launched on 4th October 1957
- In July 11, 1962 was launched the Telstar I (aT&T) was the first communications satellite
- Conclusion

The evolution of mobile telecommunications systems has been addressed in this section without going into too much detail. Additional details will be provided in the following units. We had to position the discoveries function of time but also the inventors. With mobile computing, people can work in the comfort of the place they want. In the same way, the presence of high-speed connections has also encouraged the use of the mobile phone.

Assessment

The notes provided above gives clear definitions of the terms that and abbreviations that are used in mole communication.The activity also gives the general architecture of different networks systems and their evolution.Further the learner is provided with the learning materials and assignments .

Assessments

2. One of the current trends in mobile communications is free competition, where the concept of mobility and interoperability are key. Describe the characteristics of these concepts. (2 marks)

3. What are the most common standards used in WWAN networks? (5 marks).

4. When was the mobilephones introduced in your country?What were the positive and the negative impacts on the introduction? (2 marks)

5. Describe the most appropriate mode of wireless communication that is used .List the advantages and disadvantages of the same. (5 point)

6. Describe the different types of WAN networks. (2 points)

7. Explain the concept of interoperability of mobile communications. (2 points)

8. Describe the generations of wireless (2 points)

Solution

1. Q1. For example, there is the communication of mobile phones.
2. Q2. The ability to support communication with other network type.
3. Q7. 3G is just an acronym that represents the third generation of standards and mobile technologies (3G hence the name). 3G technology improves data transmission and voice.

Reading materials and references

1. http://wireless.ece.ufl.edu/jshea/HistoryOfWirelessCommunication.html
2. Stojmenovic, I. (2002). HANDBOOK OF WIRELESS NETWORKS AND MOBILE COMPUTING.
3. Livingston, David. "Introduction & History of Mobile Computing."Slideshare. Linkedin Corporation, 5 Dec. 2013. Web. 30 Nov. 2014.
4. Wireless Networking Absolute Beginner's Guide by Michael Miller (2013)
5. Wireless Networks by Clint Smith and Daniel Collins (2014)
6. 802.11 Wireless Networks: The Definitive Guide, Second Edition by Matthew S. Gast (2005)
7. http://simplyknowledge.com/uploads/script/martincooper/Martin-Cooper-here-bg.jpg

Activity 1.2 - Radio Coverage

Introduction

Different equipments are used for wireless communication and they form a mobile network. Mobile communication can be made between different entities.for example between:

- Aircraft and ground-based system
- Vehicles
- Mobile phones
- Mobile computing equipment
- Certain classes of telemetry systems, etc.

Note that a mobile communication (eg a microwave link between a base station and a message switching center of a cellular telephone system) can be a part of the transmission that is wired, but the overall system architecture is defined as a mobile communication system. The channels associated with mobile communication systems can be grouped into two types: satellite channel and mobile

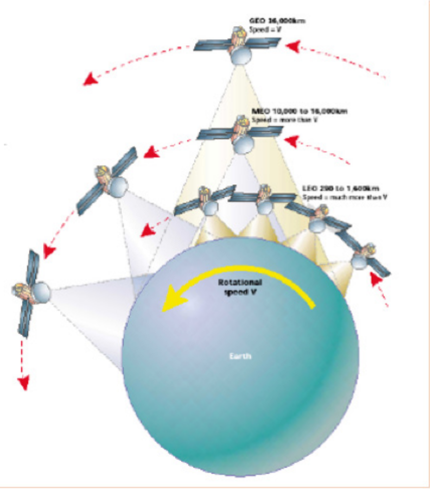
Satellite mobile communication system.

Satellite communications has been an evolving methods of providing telecommunication services and has been followed by numerous challenges.This challenges include :competition due to aggressive commercial land mobile operators,Additive white Gaussian noise(AWGN) that causes often attenuation and propagation delays of signals.

There are three categories of satellite systems:

- Geostationary orbit (GEO - Geostationary Earth Orbit) that are located 36,000 km from the earth, which means the difference between the earth's rotation and its rotation differs by approximately 0.27 seconds thus appearing to be stationary . The GEO features are:
- The transmission power of terminals and the satellite has to be strong, unless the antenna has a large diameter power.
- Satellite must have large capacity batteries to transmit at high implying large solar collectors.
- The communication trends are weak. Indeed, radio waves used being less than 20 GHz, it is difficult to have a frequency reuse as there is a strong wave broadcasting.
- The mobile-to-mobile between two stations which are not located in the same coverage area requires passage through a terrestrial network, communications between geostationary satellites being very complex. These features require the use of heavy satellites to launch expensive, while the low orbit satellites, lighter, can be initiated by small rockets .
- Satellites in medium orbit (MEO -medium Earth Orbit) which are between 1,000 and 35,700 km from the earth. These satellites take about 11 hours to circle the planet. Note that the GPS satellites are at a distance of 20,000 kms and MEO satellites are often between 13000 and 20000 km altitude.
- Satellites in low Earth orbit (LEO -Low Earth Orbit) lies at distances of 1000 km, or 700 km possible to produce smaller cells than GEO. For cells 50 km in diameter, it can be reused up to 20 000 times the same frequency. Given the proximity of the LEOs with Earth, their main advantages are a relatively low cost of launching and low transmitting power. Their major drawback is caused by displacement, since they are not stationary. .

Figure A.1.2.1 shows the different categories of satellites GEO, MEO, and THE depending on their altitude by to earth.



Radio frequency services

Radio frequencies are divided into bands, determined by a working group IEEE, DRS (Definitions of Radar standard). The band numbers and names are given by the international body of Frequency Control. Figure below shows the frequency bands allocated to satellite systems.

Mobile services correspond to ground stations that can move, that is to say having movable antennas, but at very low speeds compared those of orbiting satellites. The services offered by the mobile satellite communications and some corresponding systems can be grouped into categories:

- restricted range of services - voice and data transmission: Iridium, VSAT, Inmarsat Mini-M, ICO, Globalstar, Odyssey,Aries,Ellipso, super-GEO Multimedia:.
- broadband - Teledesic, M-Star, SATIVOD, Spaceway, Astrolink, Cyberstar, KastarKitcomm..
- message Services (store and forward): Orbcomm, GE Starsys, LEO One,
- navigation services. GPS, GLONASS, GNSS-2

Note that the VSAT (Very Small Aperture Terminal), Inmarsat (International Marine Satellite Organization), Iridium and GPS are the most popular. bands frequencies allocated to satellite

systems.Source: 2014, Olympus Satellite, the effects of the radio channel

The radio signal is attenuated as it propagates thus reducing the signal strength. We note an interference from other sources: standardized frequencies for wireless networks are shared with other devices, (eg, 2.4 GHz.) (Eg phones.) other devices (motors, microwave) interfering too. In addition, the radio signal is reflected by terrestrial objects, and signals arrive at their destination at different times where the concept of multipath . Doppler effect is also added to this problems in propagation.The Doppler effect is the perception of a frequency different from that which is transmitted by a particular source. This effect is due to the relative movement between the source and the receiver. The higher the speed of movement of the receiver with respect to the direction of propagation of the radio wave, the greater the perceived frequency is compensated.

Conclusion

Satellite systems have been a great success for the diffusion of television programs. However, the telecommunications applications that work very often with point-to-point links have much trouble finding their place in these systems.

We explore in this section the radio coverage in mobile communications. The different categories of satellites were studied. We had to show that satellite transmission suffering concepts of multipath and Doppler effect. You can continue to see the concepts covered in this section in depth through the suggested resources Questions.

Assessment

Exercise

1. Satellite channels, like all trunked systems require access technique. The essential difference with the radio interfaces of mobile networks comes from the long propagation delay between the transmitter and receiver. In cellular networks or LANs, the short propagation delay allows to easily manage the transmission instants. In the case of geostationary satellites, ground stations are discovering that there was overlapping signals 0.27 s after issue - they can listen through the distribution properties which represents a significant loss of a channel with a capacity of several megabits per second. to add to that access techniques for satellite networks are classified into four categories. What are the categories? What is the operating principle. (5 marks)

2. 2. For example Iridium refers to satellite constellations. What are the services offered by satellite constellations? What are they for ? What are the disadvantages? (5 marks).

3. What are the applications that need to use satellite services? (3 marks).

4. On the basis of three define the following satellite categories GEO, MEO, LEO. (5 marks)

5. Give the main differences between the following radio frequencies: (2 points)

   a. UHF (Ultra High Frequency)

   b. VHF (Very High Frequency

6. In which bands are GSM, GPRS, and UMTS used?

Solutions

1. The methods include fixed reservation, random access methods, packet reservation methods, and methods of dynamic reservation. for example, TDMA, FDMA and CDMA form the fixed reservation protocols.

2. The constellations allow interpersonal communication, enabling communication anytime and anywhere with terminal GSM phone sized LEOS constellations have the advantage of having a small propagation delay They require to boot.. low transmit power to reach the terminal, so that it can be used for direct communication of amobile user with the satellite. the delay due to the spread is around 10 ms, which is low compared with 250 ms for a GEOS satellite. However, the need for a large number of satellites to cover the Earth, added to the greater likelihood of having shadow areas and the increase of the Doppler effect .

3. The applications where satellite communication is the most suitable are those in which

    a. Are desirable to broadcast the same information to a destination

located

in a very large geographical area, for example, television and the Internet

    b. it is necessary want to achieve remote locations, for example, mining

camps, forestry, rural and suburban areas and highways cover

4. Here, for example the frequency to operate GSM, GPRS, and UMTS and check the corresponding band at the

References and reading materials

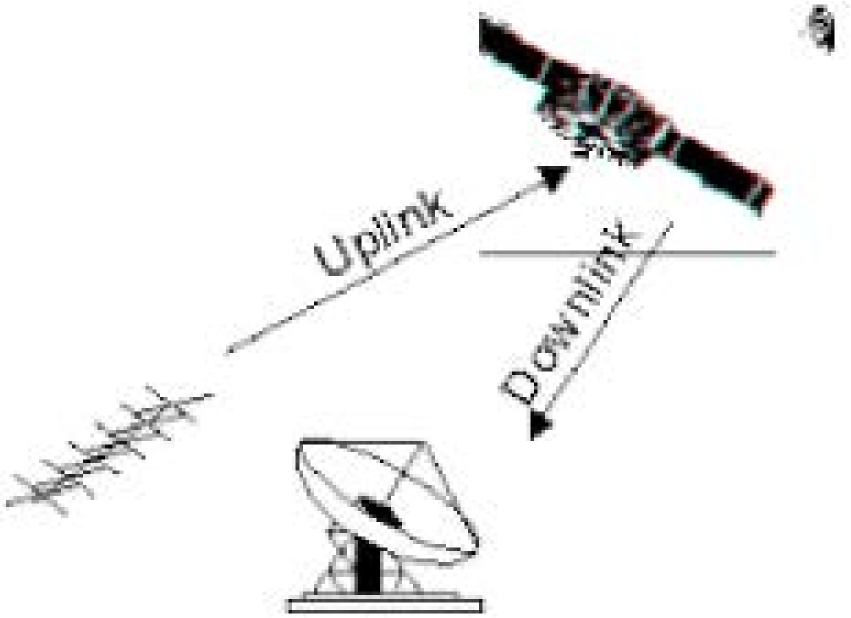
1. http://www.inetdaemon.com/tutorials/satellite/orbits/
2. http://simplyknowledge.com/uploads/script/martincooper/Martin-Cooper-here-bg.jpg
3. Designing and Deploying 802.11n Wireless Networks by Jim Geier (2010)
4. http://www.radio-electronics.com/info/satellite/communications_satellite/satellite-communications-basics-tutorial.php

Activity 1.3 - Developments and trends of cellular systems

Introduction

A handset is essential gadget for receiving / transmitting It receives and transmits radio signals. Radio communications between a transmitter and a receiver may be simplex (one-way communication), half duplex (duplex communication) or full-duplex (communication in both directions simultaneously).

The simplex transmissions or semi -duplex only requires a set of frequencies that will be common for transmission and reception. While a duplex channel requires two sets of frequencies, one for transmission and one for reception. The communication direction of a transmitter - receiver is called downlink and receiver-way communication - transmitter called uplink. To improve communication speeds in the uplink and the downlink several technology generations have the 1G to 5G.



Source: Dale Henkes, AB4NJ, "The AMSAT-NA Digital Satellite Guide – Digital Components

Frequency Plan

Mobile Communications systems use radio frequencies to transmit and receive information duplex. For example, the GSM uses [890-935 MHz] in uplink and the band [935-960 MHz] in downlink. Note the GSM 900 band was then extended to [880 MHz-890 MHz] and [925 MHz- 935 MHz] frequencies. The uplink frequency is always lower than the downlink as base frequencies undergo less attenuation in the propagation which compensates for the fact that the mobile uses a much lower power than the base station to which it connects to .

The patented cell concept in 1972 by Bell Laboratories (USA) , was the key that revolutionized mobile communications. Instead of using a high power transmitter to cover an area , it is made of different low-power transmitters which are in the same area but do not interfere with each other.

The antenna should not be installed very high and the same frequency can be reused , allowing greater coverage and allowing more subscribers . The consideration of these advantages is the need to install antennas and more extensive facilities in an increased cost of infrastructure.

Commissioning of communication cell space

This concept allows mobile frequency reuse and substantial capacity increase of traffic in the same area. Basically each of these cells may have any size , but the more appropriate format would be circular because the antenna cell is circular , if an isotropic antenna will transmit in all directions . However, in the context of mobile networks , the hexagonal cell is closer to practical reality.

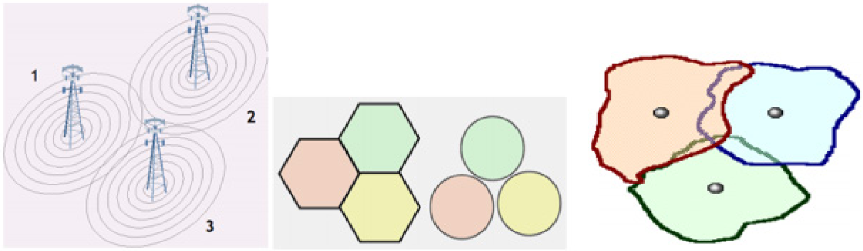


Figure A1.3.2 : Cell formats

A cell represents the geographical area covered by the radio signal(s) transmitted by the antenna (a) and communicating with mobile phones (m). When designing a cellular system , an area (cell) is covered completely by the radio signal which interferes with neighboring cells that are nearby.

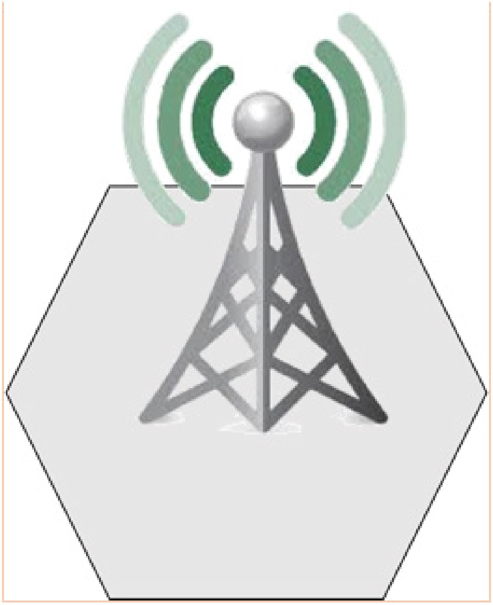


Figure A1.3.3 : Design of a cell

Concept of cluster

The cells are grouped into clusters. A cluster represents all the cells, with all frequencies available to the operator without repetition of frequencies .

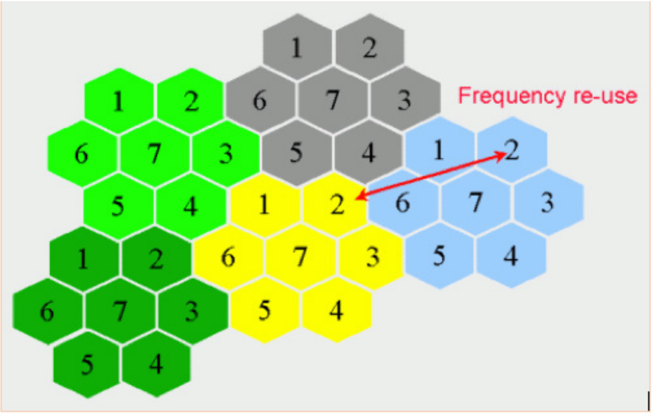
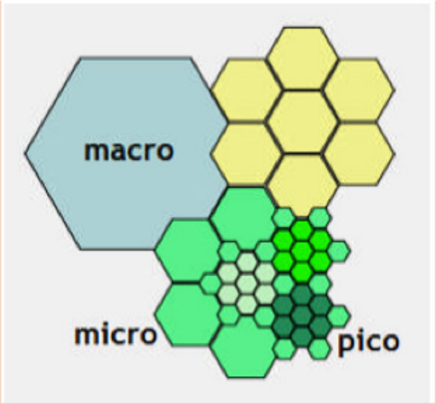


Figure A1.3.4 :Setting up clusters

Source : Felix Singo, OS12 Module

In this example, the cluster size is 7 cells for n = 7, but any value could be chosen. The most commonly used values are 3 , 4 and 7 . To make a mobile communication network project viable, the distance between the centers of clusters is a key factor to manage. Several factors, including the transmission power , the shape of the terrain / obstacles and the expected traffic volume must be taken into account. For this reason , the cell size should not be set randomly. The larger cells (macro cells) are used in low traffic areas (limited users) and spread over a larger area (eg rural areas) . These macrocells may have diameters of 3 to 35 km, although in practice they rarely exceed 10 km. In the most densely areas populated ,microcells are usually used to cover areas of streets and blocks (300m 3 km).



Implementation of Macro, Micro and Picocells

In large buildings or shopping centers, metropolitan picocells are used and they cover distances of between 30m to 300m. The transmission range is limited in the interior walls of buildings and in the neighboring cells. However, nano celles, exceptionally can be used over distances of 3m to 30m.

In addition a co-channel interference may occur. It occurs as a result of reuse by the cells of the the same set of frequencies in a given coverage.

Definition of areas

The cells are often divided into sectors, which makes them more effective. In effect, this process allows greater reuse of frequencies from which a larger number of concurrent calls. The antennas transmits the cell in sectors and split cells to cover only part of the cell not entire cell. This depends on the location of the antenna relative from the cell. The antennas may be located in the medium of cells (3) three sectors, the middle of two cells (2) or the sectors of the cell center.

Conclusion

The design of a mobile network as shown in this section and it has great advantages which can be summarized following capacity :

1. Reduction of the transmission power
2. Decentralization of all the information.
3. Address of each issue of a cell separately
4. Enable a greater number of users thanks to the reuse of frequencies already allocated .

Evaluation

Before evaluation , it will be necessary to read the notes above and master all the definitions and mobile network deployment techniques that have been developed there . Furthermore, the learner will see the suggested readings for complete documentation.

Course questions :

Q1. What are the differences between transmission simplex , half duplex and full duplex ? (2 marks)

Q2. On the basis of three criteria do you define a comparison chart between macrocell , microcell , and picocells (5 marks)

Q3. What are the frequency bands used by mobile communications in your country? (3 marks)

Q4 . What is a cluster? (2 marks)

Q5 . What is meant by the concept of “cell” in the context of mobile communications? (2 marks)

Q6 . What is homelessness? (2 marks)

Q7 . What is a BTS (Base Transceiver Station) and what is its function ? (2 marks)

Q8 . Explain what is the co- channel interference ? (2 marks)

Solutions

Q2 For example the size, deployment area, the number of users can be used as comparison criteria

Q3. free response

Q4. A cluster represents all available frequencies by the operator without repetition frequency

Q6 or roaming Roaming is a term used in mobile telephony, but also applicable to other wireless technologies. It refers to a user's ability to have a network connectivity in other different areas of the geographical location where it is registered.

Q7. The function of the BTS is to provide a radio connection to the mobile station (cell). It is mainly composed of transmitters and receivers TRX radio. It processes the signal sent by the mobile is monitoring equipment, etc. We can say that BTS is a cell within the structure of the geographical network.

Q8. Co-channel interference occurs as a result of reuse by the cells, a set of frequencies already allocated in a given coverage area.

UNIT SUMMARY

This unit has shown the evolution of radio communications since the invention of optical telegraphy by Claude Shape up the introduction of the first mobile phone by Martin Cooper . Since the first invention of the mobile phone up to date better performing phones that can send and receive data have emerged . This is possible due to the new network generations like 3G and 4G. Furthermore the propagation of radio waves and the problems encountered during transmission were shown . There has been a review study on the propagation of radio waves, including problems related to radio interference and then move to the enterprise deployment .

Unit Evaluation

Check your understanding!

Readings and Other Resources

Read the lecture notes associated with Unit 1 Read suggested readings and resources to validate all learning activities of Unit 1 resources.

Rating system

Question 1: (5 marks)

Question 2: (5 marks)

Question 3: (5 marks)

Question 4: (5 marks)

Evaluation

Question 1: To what generation to the following technologies belong: GSM , GPRS , EDGE, UMTS , HSDPA, HSUPA . Briefly describe the differences that can be observed in these technologies.

Question 2: Based on the three criteria , define a compare the following types of networks : WPAN , WLAN, WWAN .

Question 3: Describe the differences between the three categories of satellite systems.

Question 4: Explain the concepts of cells, cluster, and sectors

Question 5:Outline the concepts involved in Geostationary satellites.

Unit 2. Medium Access Techniques in a wireless environment

Unit Introduction

This unit covers the access control layer Medium Access Control (MAC), which has a crucial role in a wireless environment. It defines how different users have to share the information, the exact modalities of access in a wireless network and how to ensure good quality service. Also, the differences in infrastructured wireless networks and ad-hoc infrastructure and the creation of wireless networks are also addressed

Unit Objectives

At the end of this unit learner should be able to:

- Describe the networks infrastructure and ad-hoc infrastructure;
- Describe how the various access techniques are determined;
- Deploy an 802.11 wireless network

Key Terms

IEEE : (Institute of Electrical and Electronics Engineers) The organization aims promote knowledge in the field of electrical engineering   electronics).Legally, the IEEE is a non-profit organization under US law

LAN (LocalArea Network)

MAN: Metropolitan Area Network

WAN: Wide Area Network

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WWAN: Wireless Wide Area Network

802.11x: Set wireless network specifications developed by the LAN / MAN group of the IEEE. IEEE standards defining a wireless LAN. An 802.11 LAN is based on a cellular architecture (subdivided into cells), and wherein each cell (called Basic Service Set or BSS in the 802.11 nomenclature) is controlled by a base station (called Access Point or AP, Point french access).

irDA (infrared data association)

BSS: Basic Service Set

ESS: Extended Service Set

IBSS: Independent Basic Service Set

SSID: Service Set ID

Multi-SSID: provides multiple networks without deploying separate thread not only infrastructure:

BSA basic service area

FHSS: Frequency Hopping spread Spectrum

DSSS: Direct Sequence Spread Spectrum

OFDM: Orthogonal Frequency Division Multiplexing

SISO: Single Input Single Output

SIMO: Single Input Multiple Output

MISO: Multiple Input Single Output

MIMO: Multiple Input Multiple Output

CSMA / CD: carrier sense multiple access with collision detection

CSMA / CA: carrier sense multiple access with collision avoidance

MAC: Medium Access Control

Learning Activities

Activity 1.1 - Wireless networks

Introduction

In 1990 there was the launch of the project to create a wireless local area network or WLAN (Wireless local Area network) which aimed to provide wireless connectivity to fixed or mobile stations that required fast deployment in a local area network using different frequency bands. The first international standard for wireless local area networks was published in 2001. There were several wireless networks categories among which are:

- Wireless Personal Area Networks (WPAN)
- Bluetooth (IEEE 802.15.1) launched by Ericsson in 1994, proposing a maximum throughput of 1 Mbps to a maximum range of about thirty meters Frequency range 2.4 to 2.483 GHz and a small range because the transmission power is very low as opposed to WiFi.

- HomeRF (Home Radio Frequency) It was launched in 1998 by HomeRF Working Group (compaq, HP, Intel, Siemens, Motorola, Microsoft) proposed a theoretical speed of 10 Mbps with a range of about 50 to 100 meters without an amplifier.
- It was abandoned in 2003 at the expense of on-board WiFi (through technology "Centrino" embedding within a single component and a microprocessor WiFi adapter.
- The ZigBee (IEEE 802.15.4) provided wireless connections to very low prices and with very low power consumption. This technology was adapted directly and integrated into small electronic devices (appliances, stereo, toys, sensors, etc.).
- The infrared links were used to create wireless connections within few meters with speeds going up to a few megabits per second. This technology was widely used for home automation (remote controls) but still suffered from disturbances due to light interference. The Association IrDA (infrared data association) formed in 1995 has more than 150 members.
- Wireless local Area Networks (WLAN)
- WiFi (or IEEE 802.11),supported by the WECA alliance (Wireless Ethernet Compatibility Alliance) offers speeds up to 200 Mbps over a distance of several hundred meters.
- HiperLAN 2 (HIgh performance Radio LAN 2.0)is European standard developed by ETSI (European Telecommunications Standards Institute),which provided a theoretical speed of 54 Mbit / s over an area of one hundred meters in the frequency range between 5150 and 5300 MHz.
- DECT (Digital Enhanced Cordless Telecommunications)standard wireless mobile phones.
- The wireless metropolitan area networks (WMAN)
- Also Known as the Wireless Local Loop (WLL), the WMAN are based on the IEEE 802.16 standard the Phase 3 WiMAX offers speeds of the order of Gbit / s. This version of WiMax can be seen as an alternative to ADSL for local mobile phones).
- Wireless Wide Area Networks(WWAN)
- GSM (Global System for Mobile)communication was a special Group which originally,set the only standard used a radio frequency band around 900 MHz. It was extended to two other bands around 1800 and 1900 under the names DCS 1800 and DCS 1900 (standard used mainly in the United States). Indeed, most GSM networks use the 900 MHZ or 1800 MHZ. Some countries (Canada and USA) are using the frequencies of 850MHz and 1900 MHz frequencies 400 MHZ and 450 MHz are rarely used but particularly Scandinavian, because these frequencies were used for 1G networks
- GPRS (General Packet Radio Service) is a technique packet switching bringing the speed up to 19.8 kbit / s time slots on the 900 MHz frequency bands and 1800 MHz. This standard based on the fact that only the useful packets are transmitted, providing opportunities such as sharing resources among multiple users through an appropriate bandwidth allocation.

- UMTS (Universal Mobile Telecommunication System) uses a frequency close to a range of 2 GHz. The UMTS coverage is divided into a several of variable-sized cells. Each cell presents itself as a function of population density used and the speed of mobility.
- WiMAX (Worldwide Interoperability for Microwave Access) (standard wireless Network headed by Intel with Nokia, Fujitsu and Prowim).This is based on a frequency band 2-11 GHz, with a maximum throughput of 70 Mbit / s over over a range of 50 km , .In some places it is the major competitor with the UMTS even if it is more designed for mobile users.

The international level provides three organizations with the most weight in the wireless LAN standards are:

- he ITU-R governs the allocation of radio frequency bands
- IEEE specifies how radio frequencies are modulated to transmit information
- the Wi- Fi Alliance ensures that suppliers manufacturers of devices

shows the right standard of some wireless links based on their reach and bandwidth

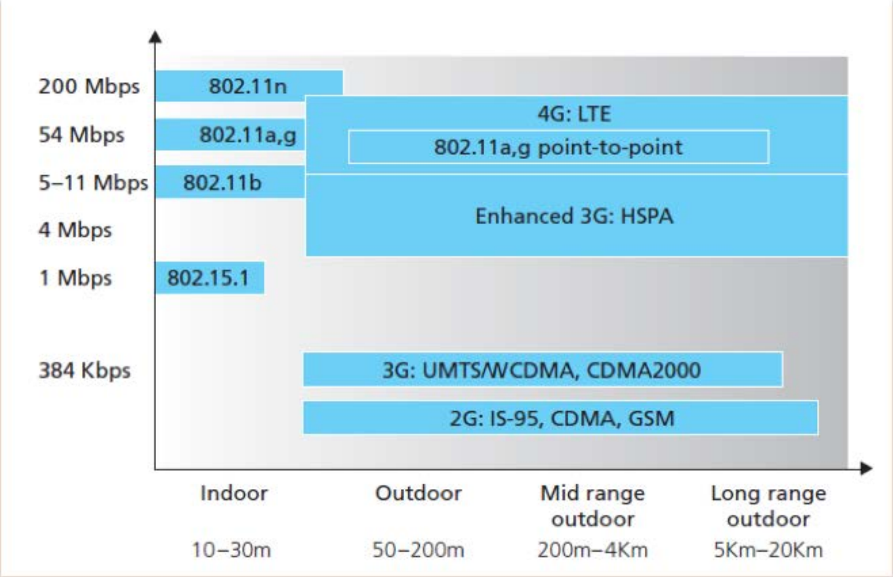


Figure Some standards of wireless links without

Extracted from: Computer networking A Top Down Approach, Kurose and Ross, 6th Edition, PEARSON, 2013.

Some wireless network applications

We are witnessing the advent expansion of smart mobile phones, smart offices and homes. Due to wireless networks In the near future there will be fully automation and connectivity within regions. Wireless technology replaces the cables.Some services are configured in a way that they recognize intruders and ,regulate temperatures

Sensor networks

Wireless Sensor Networks(WSN) are wireless network category having a very large number of nodes. They are characterized by a dense deployment and large scale in often hostile environments. These nodes are deployed around or in an area to be observed,.They are used for data acquisition and transmission to a treatment plant commonly known as "Base Station". The most important features of these nodes are their self-organizing capabilities, cooperation, speed of deployment, their error tolerance and low cost. Through the routing information protocols they are relayed by skipping between sensors to the base station. In addition, the base station through GSM, 3G, 4G or satellite can transmit data to collectors found in other networks.

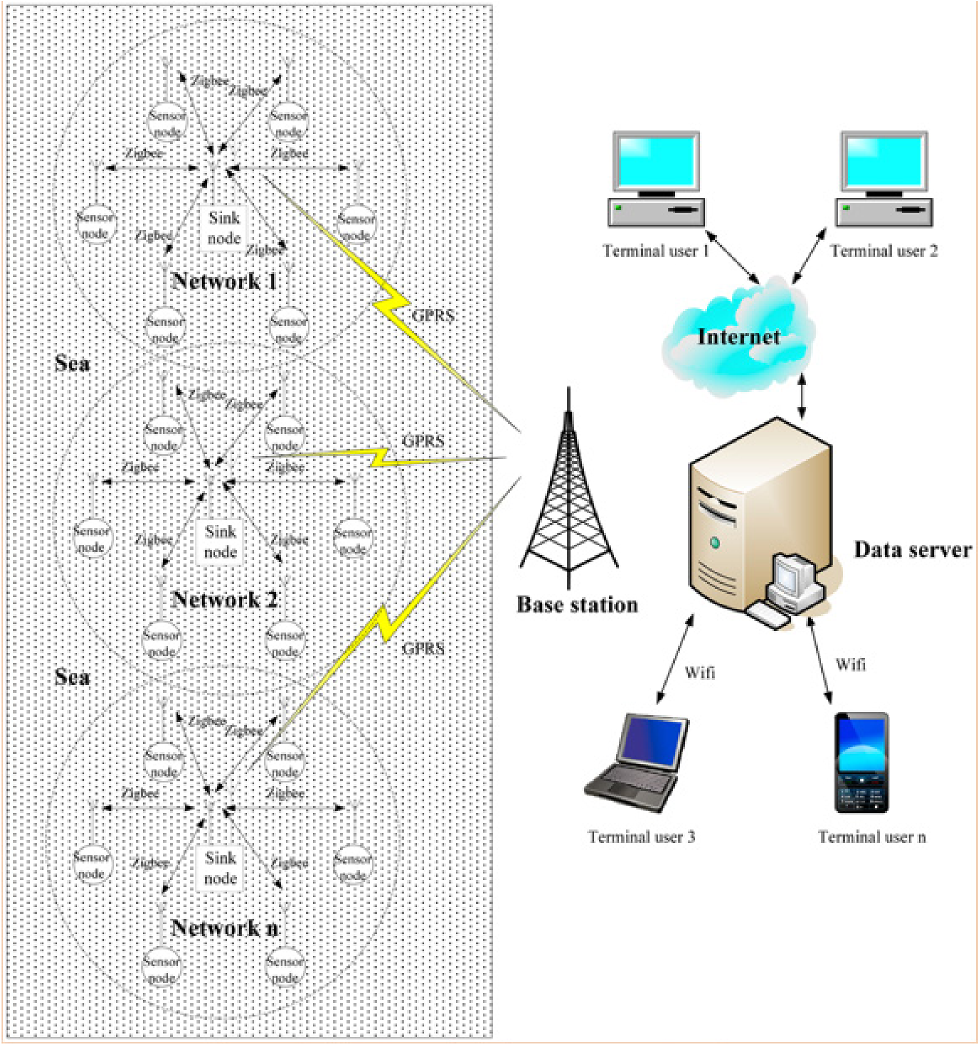


Figure Architecture of wireless sensor networks

The application areas for sensor network technology is the mostly applied in the military, the health, precision agriculture, civil engineering, security, etc. The sensors communicate with each other using ZigBee technology whose objective is to consume very little power, so that a small battery can hold almost the entire life of the interface. Figure below shows a ZigBee home automation environment speeds.

In standardization, ZigBee can have three

- 250 Kbit / s with conventional 2.4 GHz band,
- 20 Kbit / s with the band of 868 MHz available in Europe;
- 40 Kbit / s with the band of 915 MHz available in North Americafrom.

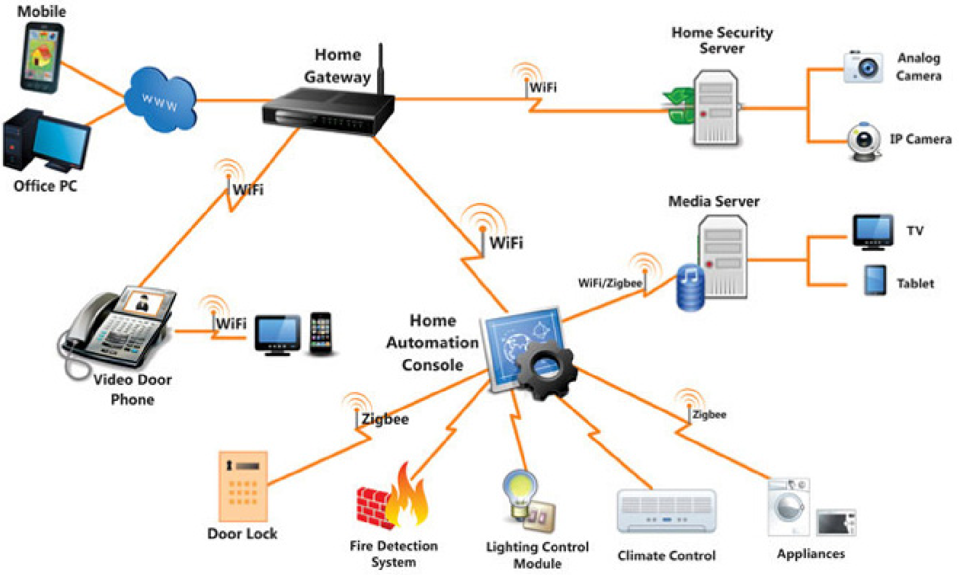


Figure A.1.1.3: ZigBee Network Automation

Extracted from Taiyito technology co. ltd

The RFID (Radio Frequency Identification)

RFID (Radio-Frequency Identification) has been introduced to achieve identification of objects, hence it is also referred to as electronic tag . Electronic tags are subjected to request by a reader, which can recover the identification information. Electronic labels are used in many applications, ranging from animal tracking tags to store. There are two main types of RFID tags: passive tags and active tags..

Passive tags do not power,they are illuminated by a reader which provides an electromagnetic field enough to generate an electric current for transmission by a radio wave by bits stored in a memory constituting the RFID.The active electronic tags have a power source in the electric component. The main advantage of these labels is the quality of the transmission. A session can be opened between the reader and the RFID so that a retransmission can be carried out automatically in case of problems. Another advantage is the transmission which ranges from several meters to the RFID and the reader, instead of a few centimeters.The transmission frequencies of RFID are indicated in the table below :

Frequency for RFID	Comment
125kHz (LF)	First solution allows a larger scope for passive RFID
13.56 MHz(HF)	most standardized frequencies used for passive RFID
400 MHz	Used mostly in detection of stolen cars
865-868 MHz(UHF)	The normalized RFID frequency used in Europe
902-928 MHz (UHF)	standard frequency band for North America
from 2.4 to 2.483 GHz5	Band free ISM in which should be used to develop many RFID applications

RFID transmission frequencies

Transmission techniques in wireless networks

There are two transmission techniques in wireless networks:

- **Infrared transmission waves (IR)**:IR uses diode to diffuse light . Infrared is used to create small networks of a few meters for example (Remote control: television,). There may be multiple reflections due to walls in offices, etc. They are used when the two devices are communicating in direct vision (line of sight). The benefits of IR transmission are: simple, cheap to implement, no need to have a license. Infrared is affected from interference due to light, heat sources, etc. Many elements absorb IR light and also have a low bandwidth. For example, the IrDA (Infrared Data Association) interface is available everywhere and has data rates up to 115kbit / s to 1Mb/s and 1Mb/s to 4 Mbit / s for 1.1waves.
- **Transmission by radio** It is used mainly in tape ISM frequencies (Indrustrie Science Medicine). Indeed, ISM band includes three sub-bands: 900 MHz, 2.4 GHz, and 5GH and is not subject to international regulations. It can be used freely for the needs of industry, science and medicine. Radio waves are used in wireless networks and mobile telephony. They can cover wider areas since the radio can penetrate walls. The drawbacks to note are the limitation of the frequency band and the interference with other equipment.

Conclusion

Wireless networks have become a growth market in the twenty-first century. Mobile telephone terminals have been the big winners in the late twentieth centuery, but they are not vested as telephone communications. Indeed, wireless networks provide high data rates, enabling a PC or a wizard to connect without worrying about wiring and even slow connection provided you do not go out of its coverage area. Sensor networks and RFID technologies are revolutionizing the world with the Internet of Things. Everything will be connected in the coming years. The ZigBee solution is on track to become an industry standard of WPAN networks.

Evaluation

The notes above are meant for the definitions and network architectures that have been developed there. Furthermore, the learner will necessarily consult the suggested readings for complete documentation.

Multiple Choice Questions

1. What are the characteristics of a sensor in a sensor network? (2 points)

   a. Two sensors with different processors can not communicate with each other.

   b. The sensors have strong memory constraints.

   c. The sensors have strong processor capabilities.

   d. The sensors can detect only the temperature.

2. What are the characteristics of RFID? (2 points)

   a. An RFID tag consists of a microchip and an antenna.

   b. The RFID chip has a unique identifier.

   c. A RFID chip sends its information all the time.

   d. An RFID chip includes a mini battery.

3. Why does network sensors a limited lifespan? (1 point)

   a. They are fragile

   b. The material is not very reliable, we know that failure often

   c. they rely on batteries that do not plan to change issues:...

current

1. Basing on the criteria compare the following categories of wireless networks WPAN, WLAN, WWAN. (5 points)

2. Q2. Why is Bluetooth scope limited to only a few meters? (2 points)

3. Q3. Give the differences Mobile WiMAX and WiMAX (2 points)

4. Q4. What is ZigBee? (2 points)

5. Q5. What are the advantages of radio transmission from the infrared transmission. (2 points)

6. Q6. On the basis of the three criteria how do you define a comparative table of ZigBee and RFID (3 points)

7. FeedBack

1. This is because of the power transmission.

2. The comparison criteria are: frequency, rate, range802.11.

Activity 1.2 - MAC

1. **The basic components of a wireless network**

Figure A.1.2.1 shows the different elements of a wireless network. The elements that make up the wireless network in this situation are:

- The wireless host (PC, PDA, IP phone)
- The base station (Wireless Access Point) is the relay responsible for sending packets between wired and the host of a wireless area.
- The wireless links that are usually used to connect the mobile to the base station. There are many access protocols that coordinate access to and link with different transmission rates.
- The mobile may be in motion and change base station. This is represented by the concept of "wireless host in motion" in the Figure below..

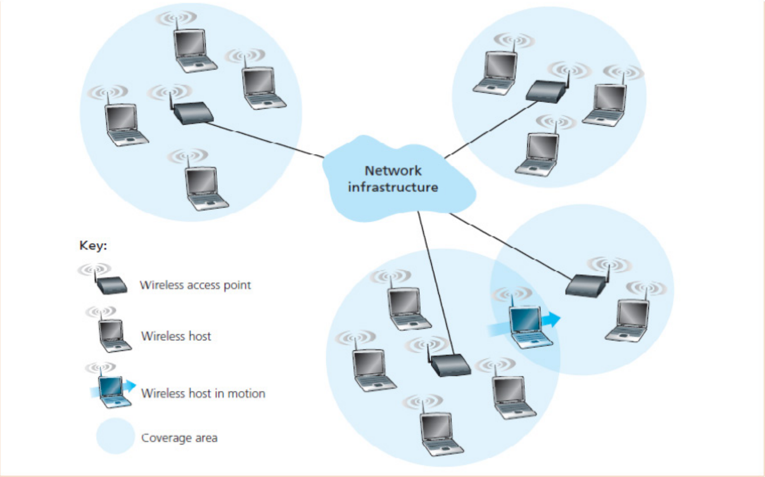


Figure The elements of a wireless infrastructure network

Extracted from: Computer Networking A Top Down Approach, Kurose and Ross, 6th Edition, PEARSON, 2013.

2.1 802.11 architecture

a) infrastructure mode

Figure A.1.2.2 shows the different components of an 802.11 wireless network. The main element of the 802.11 LAN architecture is the BSS (Basic Service Station). When one is in infrastructure mode, the BSS contains a single access point and the stations associated with this access point. The communication must go with the access point.

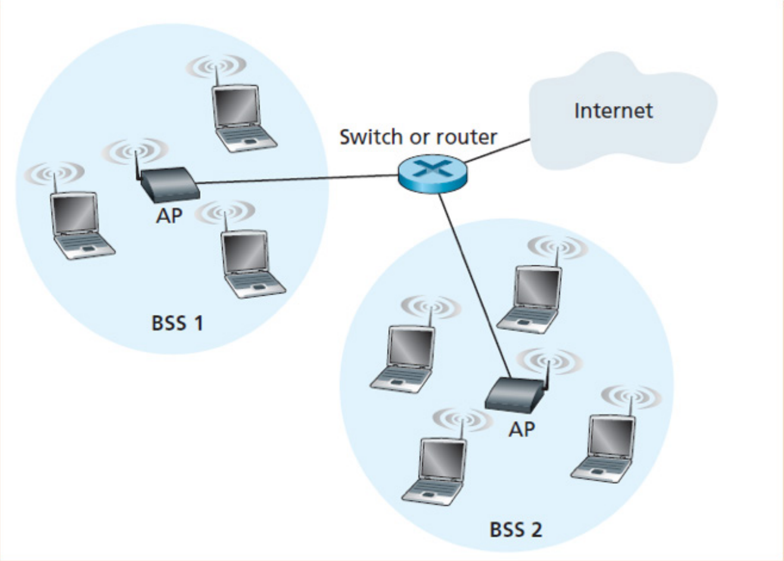


Figure A.1.2.2: Architecture LAN 802.11

Extracted from: Computer Networking A Top Down Approach, Kurose and Ross, 6th Edition,

An alternative is a grouping of several BSS where the access points are interconnected by a distribution system. This set is called ESS (Extended Service Set). Figure A.1.2.3 shows the case of such an architecture when in infrastructure mode

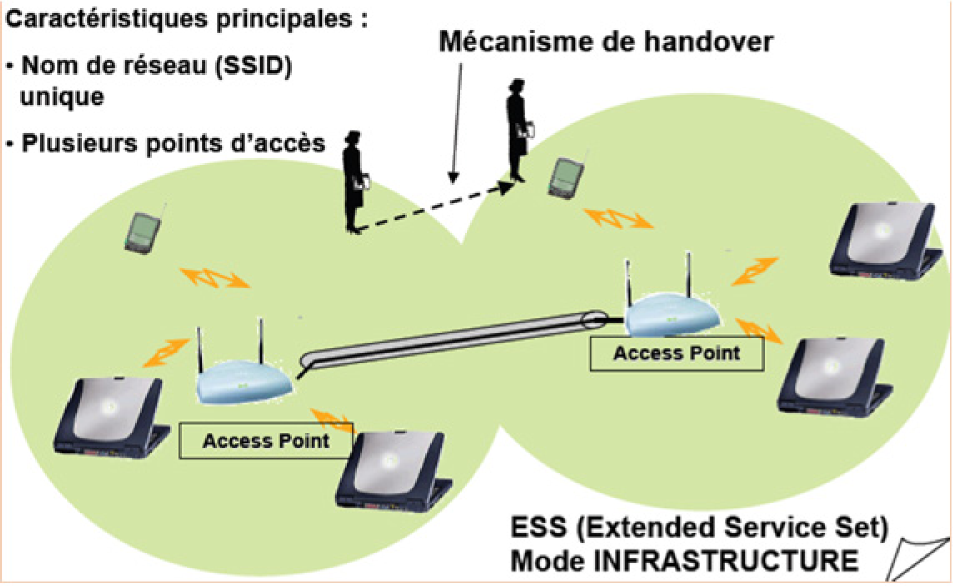

Caractéristiques principales :
• Nom de réseau (SSID) unique
• Plusieurs points d'accès
Mécanisme de handover
Access Point
Access Point
ESS (Extended Service Set)
Mode INFRASTRUCTURE

Figure A.1.2.3: 802.11 LAN architecture: ESS

b) ad hoc mode

In this mode there is no base station. Therefore only the nodes transmit to other nodes within the wireless coverage. the nodes are organized in a form of network. It is mandatory to have a routing system in them. In this case of routing protocols that can be reactive, proactive or hybrid. If we have a set of BSS in ad hoc mode, the set obtained is representedi n IBSS (Independent Basic Service Set). Figure A.1.2.4 shows the case where we have an IBSSA.1.2.4.

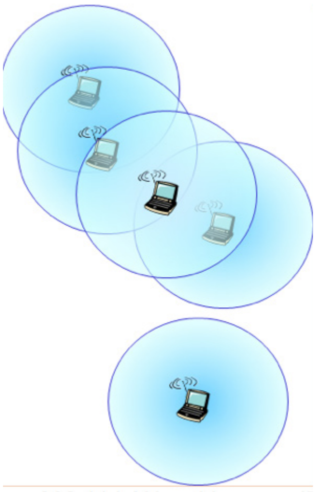


Figure 802.11 LAN architecture: IBSS

WiFi: 802.11 Wireless LAN

There are various 802.11 standards including 802.11b, 802.11a, 802.11g, 802.11 No, 802.11ac. These standards have the following characteristics below:

- 802.11b uses frequency between 2.4GHz and 2,485GHz with a max speed of 11 Mbit / s
- 802.11a uses the frequency band between 5, 1GHz and 5.8GHz with a maximum flow 54 Mbit / s
- 802.11g uses the frequency band between 2.4GHz and 2,485GHz with a max speed of 54 Mbit / s
- 802.11n uses the frequency band of 2.4GHz or 5GHz with a max speed of 200 Mbit / s and uses multiple transmitter antennas and multiple antennas for reception. This is the concept of MIMO (Multiple-Input Multiple-Output). 802.11n products are often single band, usually at 2.4GHz (for reasons of production cost). However one can have “WiFi b / g / n” (or “WiFi a / n”) for single band or label “WiFi a / b / g / n” for dual band.

Note that all standards can operate in infrastructure mode or ad hoc mode While recently in 2014. There was the development of:

- 802.11ad is a new generation of WiFi called WiGig and uses the 60GHz frequency band at a rate between 1Gbit / s and 6Gibit / s was standardized by the IEEE group "very high throughput." However the 802.1ad is more oriented to PAN LAN.
- 802.11ac uses only one frequency band of 5 to 6 GHz with a speed of up to 7 Gbit / s. 802.11ac also uses the MIMO

Technique..

The 802.11 MAC protocol

When an administrator installs an access point there is assignment of a communication channel to each access point. Note that some access points can allocate channels dynamically to users. Europeans access points possess usable channels 1 to 13 and those channels for Americans range from 1 to 11. The channels range from 2.4GHz to 2,485GHz and it is in this 85 MHz band that different channels are assigned . Each node must associate to the access point that , choose a communication channel. To discover the communication channel there are two methods: either a passive or active search)..

- In the "passive search", the node senses all channels to retrieve tags frames (if These tags frames are sent by the access point. Then, the recovery of a main frame that contains the information of connecting to the access point, the node selects a channel based on the signal / noise ratio
- in "active search",mode the node sending a message Probe a Request on available channels. The access points are located in the vicinity of response through a Probe Response. Then, recovery of the frame tag choosing a network is made or when the node knows the desired network.

Once the node is associated with the access point, it pends to send and receive data . Given that multiple nodes can simultaneously send data on the same communication channel, there may be collisions. It is necessary to have multiple access protocol to regulate access to the media. In the literature there are three major multiple access protocol families: partitioning, random, and each turn. Given that there was already a random access protocol called CSMA / CD for Ethernet, 802.11 is is inspired. by collision, a station must be able to listen and transmit simultaneously. In radio systems, transmission covers the reception of signals on the same frequency and does not allow the station to experience the collision: radio links are never full duplex. As a station can not get its own transmission, if a collision occurs, the station continues to transmit the entire frame, resulting to a loss of network performance. The access technology Wi-Fi must take account of this phenomenon therefore a new MAC protocol called CSMA / CA was created.

802.11 5.1 data link layer

It consists of two sub layers:

- The under layer LLC: Logical Link Control that uses the same properties as the 802.2 LLC layer. So avnos us the ability to connect to a WLAN other premises belonging to a network standard IEEE
- The MAC layer: Medium Access Control that is specific to IEEE 802.11. As against it is quite similar to the 802.3 MAC layer of the Earth's Ethernet network.

The LLC layer is defined in the 802.2 standard, and plays a logical connection between the MAC layer and the OSI model network layer through the LSAP (Logical Service Access Point). The role of the LLC layer is to manage the flow control and error recovery. The LSAP helps make interoperable different networks with MAC or physical, but with the same LLCA.1.2.5.

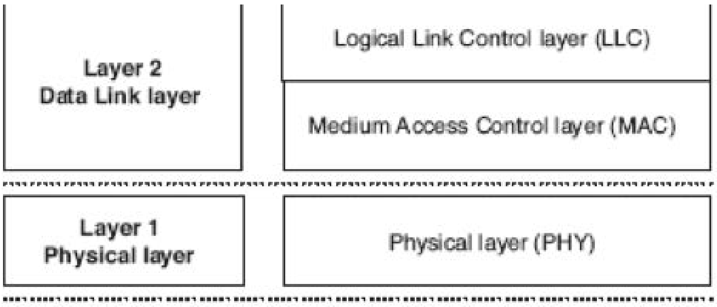

Layer 2
Data Link layer
Logical Link Control layer (LLC)
Medium Access Control layer (MAC)
Layer 1
Physical layer
Physical layer (PHY)

Figure The data link layer

At the Figure A.1.2.5, the LPDU (Logical Data Protocol Unit) represents the data of the LLC frame that is encapsulated in the MAC frame when the MPDU (MAC Protocol data Unit) is the

MAC frame which encapsulated in the physical layer.

802.11 MAC layer

802.11 MAC provides the following :

- Media access control
- Addressing and formatting of frames
- Error check CRC (Cyclic Redundancy Check)
- Fragmentation and reassembly (high error rate because of the 802.11)
- Quality of Service
- Energy Management
- Mobility management
- Security
- Two access methods:

- DCF (Distributed Coordination Function): It is quite similar to traditional network supporting the Best Effort and is designed to support data transport asynchronous.users who want to transmit data have equal opportunity to access support from which the limited probability to have collisions Function).
- PCF (Point Coordination) There is no contention and no collisions because the access point requests in turn the terminals. The transmission control nodes is centralized at the point of access. This access technique is designed for the transmission of sensitive data (synchronous) who need to manage the transmission delay and the real-time type applications (voice, video, etc.)

802.11 All implementations are supported by DCF, as opposed to the PCF which is optional. Note that in an ad hoc network only the DCF mode is supported.

The CSMA / CA protocol

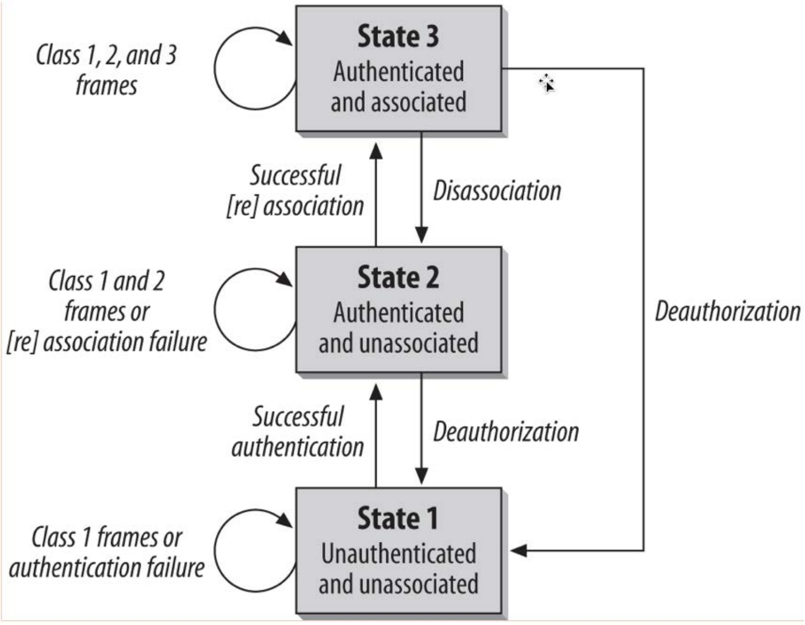
Since it is impossible to detect collisions, should be avoided. The CSMA / CA protocol provides four mechanisms. Use positive acknowledgment of reception, timers for the reservation, listening support (VCS mechanisms and PCS), back-off algorithm

CSMA / CA avoids collisions by using acknowledgment frames or ACK (Acknowledgement). ACK is sent from destination station to confirm that the data is received on intact. The media access is controlled by the use of interframe spaces, or IFS (Inter-Frame Spacing), which correspond to the time interval between the transmission of two frames. IFS intervals are periods of inactivity on the transmission medium. Values of different IFS are calculated by the physical layer. The standard defines three types of IFS:

- SIFS (Short Inter-Frame Spacing), the smallest of the IFS, is used to separate transmissions within the same dialogue (sending data, ACK, etc.). There is always one station to transmit at any time interval, thus having priority over all other stations. The value of the SIFS is 28 microseconds.
- PIFS (PCF IFS),is used by the access point to access with priority of support. PIFS is the value SIFS, to which is added a time, or time slot is defined in the back-off algorithm, of 78 microseconds. Note that the algorithm has to Back-off for one of them nodes Present in collisions.
- DIFS (DCF IFS) is used when a station wants to start a new transmission. The DIFS is the value of PIFS, to which is added a time of 128 microseconds.
- EIFS (Extended IFS is the only used for retransmissions upon receipt of a bad frame (CRC or collision)

The terminals one BSS can sense the activity of all stations located there.When a station sends a frame, other stations fit avoid avoid a collision, The update of a timer, called NAV (Network Allocation Vector) is liable for delaying all planned transmissions. The NAV is calculated in relation to information located in the lifetime field, or TTL, contained in frames that have been sent. Other stations have the ability to pass after the end of the NAV. Indeed, the NAV is actually a timer that determines the timing at which the frame can be transmitted successfully.

A source station wishing to transmit data support sensing. If no activity is detected for a period of time corresponding to a DIFS, it transmits its data immediately. If the media is still busy, it continues to listen until it is free. When the media becomes available, it still delays its transmission using the back-off algorithm before transmitting their data. If the submitted data is received intact, the destination station waits for a time equivalent to a SIFS and sends an ACK to confirm their good reception. If the ACK is not detected by the originating station or if the data is not received properly or if the ACK is not received correctly, it is assumed that a collision has occurred, and the frame is sent


Class 1, 2, and 3 frames
State 3
Authenticated and associated
Successful [re] association
Disassociation
Class 1 and 2 frames or [re] association failure
State 2
Authenticated and unassociated
Deauthorization
Successful authentication
Deauthorization
Class 1 frames or authentication failure
State 1
Unauthenticated and unassociated

FigureA.1.2.6.frame transmission process

Extract of: Guy Pujolle, Networks, Publishing 2008 Edition Eyrolles, 2008

When the source station transmits its data, other stations update their NAV, including the time of transmission of the data frame, the SIFS and the ACK. Figure A.1.2.6 shows the frames of the transmission process from a transmitter. This process includes the different expectations than just detailed.

CSMA / CA back-off

It solves the problem of media access when many stations want to transmit data at the same time time. The random selection of backoff is performed in an interval called the contention window (CW: Contention Window). The size of this window depends on the number of transmission attempts. Its size is doubled each unsuccessful attempt. Each failure shows that the spread of the requests in time was not important enough. The draw must take place on a larger interval. Each attempted transmission, the timer carries out the following trends :

- [2 2 + i *randf ()] * timeslot with
- i is the number of consecutive attempts for a station to send a frame ,
- randf () is a variable between 0 and 1.

Using this algorithm, the stations have the same probability of accessing the media. Its only drawback is that it does not ensure minimal delay and thus complicating the management of real-time applications such as voice or video. Note that the contention window returns to the initial state when the node transmits successfully its frame.

Reservation RTS / CTS and the problem of the hidden station

In Wi-Fi, detection the media is both at the physical layer, with the PCS (Physical Carrier Sense) and at the MAC layer , with the VCS (Virtual Carrier Sense) . The PCS detects the presence of other wireless stations by analyzing every frame from the wireless carrier and detecting the activity on the support due to the relative signal strength of all stations.

The VCS is a booking mechanism based on sending frames RTS / CTS (Request to Send / Clear to Send) between a source station and a destination station before sending data. A source station that wants to transmit data sends RTS . All BSS stations detecting the RTS read the TTL field of the RTS and update their NAV . The destination station having received the RTS meets after have waited for a SIFS , sending a CTS . The other stations detecting the CTS read the duration field of the CTS and put again to update their NAV . After receiving the CTS by the source station , it is ensured that the support is stable and reserved for its data transmission.

This allows the source station to transmit data and receive ACK without collision. As the RTS / CTS frames reserve the medium for the transmission of a station , this mechanism is typically used to send large frames for which retransmission would be too costly in terms of bandwidth. Figure A.1.2.7 shows the issuance process of a frame when the destination station is hidden.

Stations can choose to use the RTS / CTS mechanism or use it only when the frame to send exceeds a RTS_Threshold variable or never use it.

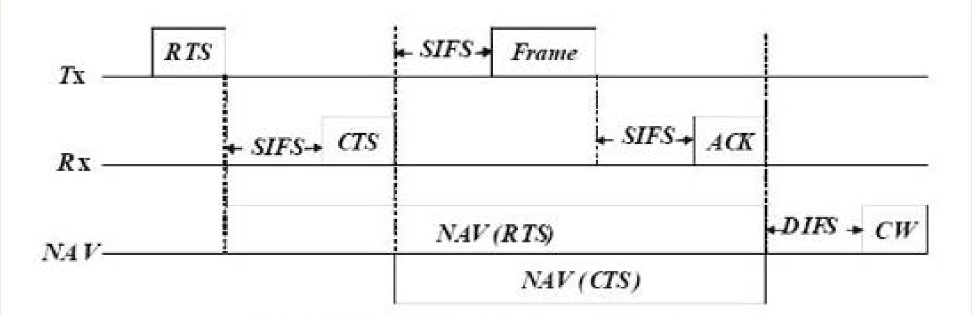


Figure 4. RTS/CTS protection mechanism

Figure A.1.2.7 reservation mechanisms RTS / CTS

The fragmentation and reassembly

The error rate for wireless connections is much higher than wired connections which requires the transmission of small packets . We can break the frame if it exceeds a threshold value . By usingRTS / CTS booking mechanism is used only the first fragment uses the RTS / CTS frames . As against the NAV should be kept updated with each new fragment

Conclusion

The CSMA / CA protocol enables to share access . The acknowledgment mechanism also supports effectively Interference Problems and generally all the radio environment issues. The reservation mechanism RTS / CTS avoids the problems of the hidden station . All these mechanisms , however, result in the addition to Wi-Fi headers frames that Ethernet frames do not possess. This is why wireless networks always show lower performance than Ethernet LANs .

Evaluation

The question below are meant to examine the understanding of different protocols used in wireless communication systems

Questions de cours :

1. Why is the effective throughput of a wireless network it is diferent r from theoretical throughput? (1 point)
2. Outline the functioning of Wi-Fi network working at the speed of 11 Mbit / s. (5 marks)
3. If 11 clients share the resources of a cell, each user why dose each client receive not more than 1 Mbit / s on average?(5 marks)
4. What can be the maximum theoretical throughput in a cell?
5. A customer capturing the signals of two access points should select the access point to which it will connect. In your opinion, how is selection done ?

   If an 802.11b access point is located in the same place an access point 802.11a,

   what is impact on the throughput?(5 marks)
6. If two clients access the same access point with different speeds (eg, one to 11 Mbit / s and the other at 1 Mbit / s, how fast must the access point issue its supervisory frames?(5 marks)
7. If a Wi-Fi card could automatically transmit at sufficient power to reach the access point, would it lengthen the battery life time?(3marks)
8. What makes up a BSS and what is it identified (name and format or password) ? (1 mark)
9. What ESS and how is it identified ? (1 point)

Activité 1.3 The deployment of a wireless network 802.11

Introduction

The higher the power , the greater the range of the signal , the greater the waves pass through obstacles. To double the signal strength , you have to quadruple the power of the transmitter . However, when talking about " quadruple power " of the issuer, it is the power expressed in Watt .

Thus , lower frequencies have greater range and better through the obstacles. A power equal emission , radio waves at 2.4 GHz are about twice as far as wave 5 GHz. However, the legislation allows for powers from 200 to 1000 mW for 5 GHz while the limit is only 100 mW for the 2.4 GHz , which compensates the difference

1. The radio report

For a wireless communication to take place, we need the radio report is satisfactory in both directions. A margin of 6 dBm is generally considered the minimum to ensure a stable connection required for the antenna cables as short as possible and receiver sensitivity as good as possible .It is Better to have high gain antenna (which acts both in reception and transmission) rather than a powerful transmitter. EIRP, which is the equivalent isotropic radiated power of a system is equal to the power of the transmitter, plus the antenna gain, the greater the loss in the antenna cable and connectors is also limited!

To realize the radio report there are required tools. The easiest way to travel with a laptop or PDA and use the tools provided with the sound driver WiFi adapter to measure signal quality. We can then note where are any gray areas and move the AP to find an optimal configuration

The free tool "Network Stumbler " is another solution is to perform the audit site with Netstumbler analysis tool , free download www.stumbler.net .

Specialized commercial software in the site audit are numerous. We can mention : AirDefense , AirMagnet , Finisar , Network Associates, and WildPackets YellowJacket . In addition to the parameters indicated by NetStumbler (signal level , SNR , channel , SSID , BSSID) , the software can obtain many other important information:

- The actual flow rate through an "active" mode is which the software joins the wireless network and performs data transfers with itself , so without the need to connect the AP to the wired network

2. Planning to achieve proper planning must be taken into account depending on the following aspects :

It depends on the geographical structure of your system (number of entities and devices present in a space). It depends on the expected data rates by the users (since the radio frequency is a shared medium , the more users there are , the more conflicts of use of radio frequencies are important). It depends on the use of non-overlapping channels through multiple access points present in a range of extended services , as well as transmission power settings (which are limited by local regulations)

- Placement of access points:

Move to the extent possible the AP (Access Point) above obstacles

Position the AP vertically near the ceiling and the center of each coverage area, if possible

AP to be installed in locations where users are required to work

For example, the conference rooms are often a more appropriate location for the access points as hallways. When these have been resolved , evaluate the expected coverage area of each AP

- Assigning cannaux

If two access points using the same channels have emission zones overlapping , signal distortions may disrupt the transmission. So to avoid interference it is recommended to organize the distribution of access points and channel usage in a way not to have two access points using the same channels close to each other. Figure below shows an example of assignment to 7 access points 3 channels that do not interfere with each other . We have another possibility through an access point where 11 channels are available: Channel 1, Channel 6 and Channel 11

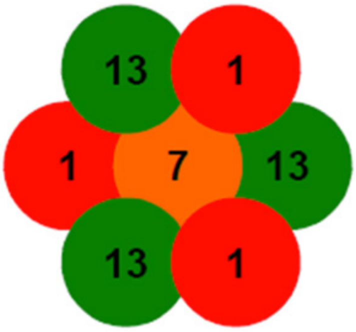


Figure A.1.3.1

channel assignment

Conclusion

To have a good quality of service in wireless 802.11 network it is mandatory that the radio is satisfactory balance between nodes and or access points. It will secondly evaluate the coverage area of your access point and avoid interference between access points at the deployment site .

However, wireless networks are well established and their success is undeniable . The new 802.11 standards allow increased flow , secure transmissions and a better quality of service.

Evaluation

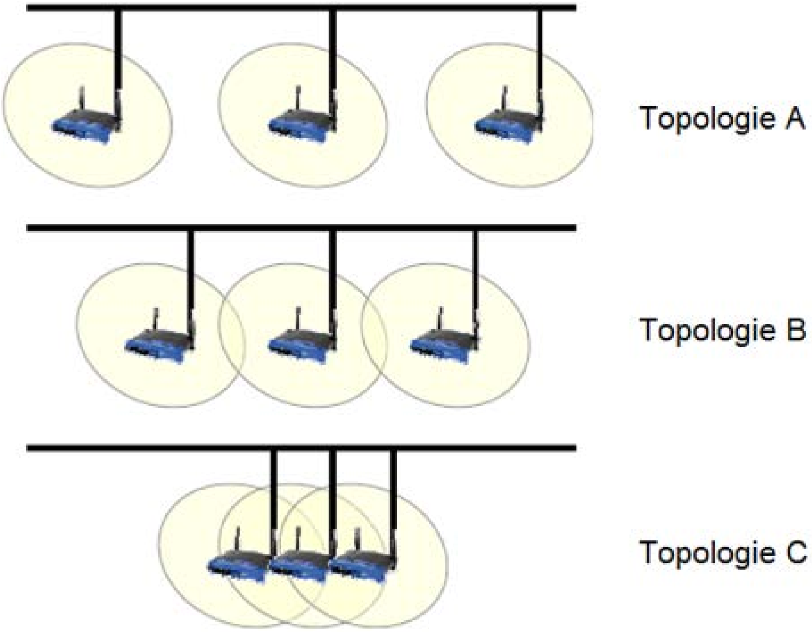
The above mentioned topics are meant for definition and mastering of 802.11 technology .More materials are provided for deeper understanding of the contents.

Questions de cours

1. You would like to install an 802.11g access point which 13 channels are available. You detect the presence of another access point which uses channel 4 What would be the effect on the performance of your WLAN :Also if you choose channel 4 (explain) ? (1 point) if you select channel 5 (explain) ? (1 point) if you select channel 13 (explain) ? (1 point)

Exercice 1

Compared to the proposed topologies below give the advantages and disadvantages compared to interference, the number of users , the impact of the channel assignment .



1. Exercice 1

a. for the Topology A since the cells are disjoint we have a low number of channels, no interference , no mobility

b. for the Topology B because the cells overlap, we have a wireless network , a mobility service , the use of space , the management of the assignment.

c. for the topology C , because the cells overlap each other a channel configuration is necessary and this topology allows a large number of users

UNIT SUMMARY

Basic Wi-Fi networks from the IEEE 802.11b standard on the tape

2.4 GHz . As explained above, this standard originates studies

conducted within the general framework of the 802.11 group. Wi -Fi network extensions were made by the standardization IEEE 802.11a, IEEE 802.11g , IEEE 802.11n , IEEE802.11ac .

The 802.11 MAC layer implements the CSMA / CA protocol which firstly manages multiple access to the support and the other with his back-off algorithm tie knots colliding . Note that there is a RTS / CTS reservation mechanism to avoid collisions and the problem of the hidden station.In addition to an improved quality of service , should therefore , when engineering the network , while calculate the positioning of the various access points. Note that the frequencies can be reused regularly if well spaced

Directives

1. Read the lecture notes associated with the Unit 2
2. Read suggested readings and resources
3. Validate all learning activities of the Unit 2
4. Study on the 802.11 MAC protocols and pre required to deploy a WiFi network.

Readings and Other Resources

Readings and other resources for this unit are level readings and other course resources.

List of relevant readings :

Play # 1: Guy Pujolle , Networks , Publishing 2008 Edition Eyrolles, 2008

Justification : Consultation of Chapter 22 personal networks Bluethooth , UWB , and ZigBee allows to become familiar with new trends PAN networks . Reading this chapter provides insight into the operation of sensor networks and RFID technologies. s reasons for the transition from 1st generation to 3rd generation or 4th generation mobile networks.

Unit 3. Systems and wireless telephony standards

Unit Introduction

This unit allows to gain knowledge on the different generations of mobile networks and wireless telephone networks. It discusses in detail the generation mobile network GSM, GPRS, EDGE, LTE and CT0 generations, CT1, CT2 cordless telephone, and operation of the DECT (Digital Enhanced Cordless Telecommunications) which defines an air interface technology for . Wireless telecommunications

key Terms

ETSI. (European telecommunications standards Institute), that is to say, the European telecommunications standards Institute is the standards body European area of telecommunication

IMT-2000. (International Mobile telecommunications for the year 2000) is the acronym chosen by the ITU to designate five radio access technologies for cellular systems of the third generation

ISDN. Integrated service for Digital network .

DVB: Digital Video broadcasting (Standards defined by ETSI for digital TV broadcasting)

(Cable- 1993) digital television broadcasting with a maximum speed of 38Mbps and a transmission channel the less disruptive

DVB-T (terrestrial- 1997) terrestrial radio channel disrupted with the same bands as analog **TV (UHF),** the same cellular system that analog TV and a 30 Mbps theoretical throughput (in practice: 5 to 20 Mbps)

DVB-H: (Hand -2004) is a transmission used by small mobile device battery new constraints compared to DVB-T: increase the battery usage durrée and using different frequency bands and rates of 5 to 32Mbps

DVB-S. (Satellite - 1993) is a geostationary satellite transmission with a simpler transmission channel DVB-T and theoretical speeds of 24 to 40 Mbps(Satellite.

DVB-S2 - 2004) is a DVB-T extension with theoretical speeds of 80Mbps DVB.

DVB-RCS (return Channel Satellite - 1999) We have a return channel (user -> transmitting station) for interactivity and reception via -S, and transmission to the satellite by the same antenna. This transmission can be used for broadband Internet for remote areas not served by **ADSL**. Nudes have a return path on speed: 2 Mbps amount 8Mbps down roaming).

Roaming (or Allows the network to transmit a call (incoming call) while the appellant has no knowledge of the geographical position of the called network.

TDMA (Time Multiplexing Access Division)- temporal Multiplexing

FDMA (frequency Multiplexing Access Division) - frequency Division Multiplexing

CDMA (code Multiplexing Access Division) - Spread spectrum (division by code)

AMPS (Advanced Mobile Phone Service) in the US (Chicago, AT & T, 1979); 1 global system subscribers until 1997

Network NMT (Nordic Mobile Phone) Sweden (Ericsson, 1981)

Network TACS (Total Access Coverage System adapted from AMPS

to 900MHz) in UK (Vodafone, former Racal Telecoms 1985)

RADIOCOM Network 2000 (450MHz) in France (France Telecom, 1985)

DECT(Digital European Cordless Telecommunications) - European standard for digital voice radio point to point between a phone or a light portable terminal and a station based. The **DECT** standard provides for the transfer = inter cell roaming)1995).

IS 95: US second-generation system:

PDC Japanese second generation system

PHS: Personal Handset System (replaces the pager; no cell; Low tariff at high speed (64 kbit / s) limited

CT2 mobility. digital radio standard wireless. CT2 defines small handheld devices for calling communicating through intermediate terminals located a few hundred meters, but not receive

GSM. GSM: TDMA-based, standard originated in Europe but used worldwide

GSM / IS-54 mobile phones 2nd generation PCS. (Personal Communication system)

CDMA 2000 standard to supplant American CDMA-One system. allows data rates up to 140 kbits / s

UMB. (Ultra Mobile Broadband) proposed by Qualcomm to improve the CDMA2000 but was abandoned in November 2008 in favor of LTE

GPRS. packet switching technique on GSM. Mobile telecommunication network to packet switching. GSM Evolution for transmitting packet multimedia data, at high speeds, in the context of existing radio infrastructures

MSC. (Mobile Service Switching Center). It is responsible for routing in the network, interconnection with other networks (conventional telephone network, for example) and coordination of the calls. MSC processes the "voice" traffic and signaling several BSC

BSC. (Base Station Controller) it controls a set of BTS (up to several hundred)

EDGE. (Enhanced Data rate for GSM Evolution) is an evolution GPRS standard is available since 2003 and allows data rates up to 230 kbit / s

UMTS.(Universal Mobile Telecommunications System) is the evolution of GSM to provide 3g Services.

HSPA (High Speed Packet Access) is a generic term adopted by the UMTS Forum to name the improvement of UMTS radio interface. HSPA mean enhancements to both the downward flow (HSDPA) and upflow (HSUPA). As part of the evolution of GSM to 3G, HSPA enables faster data transfer, to enhance spectral efficiency and increase the capacity of operators of systems. Regarding users, HSPA provides access to a world of mobile high débitmultimédia

HSDPA. (High-Speed Downlink Packet Access) Evolution of UMTS that advances the receipt flows (in the direction towards the network terminal) to 2 Mbit / second (and, if one believes handset providers; 3 Mbps and up to 14 Mbit / s

LTE. (Long Term evolution) is the evolution dde HSPA Mobile.

IMSI (International Subscriber Identity) is a unique number that allows a mobile network GSM, **UMTS** or LTE to identify a user. This number is stored in the SIM card (USIM in UMTS and LTE) and is not known to the user . to achieve this, the operator assigns a MSISDN which is the version with international prefix of what is commonly called a "mobile phone number"card.

SIM (Subscriber Identity Module) is a chip containing a . microcontroller and memory and is used in mobile phones to store information specific to a subscriber of a mobile network, especially for GSM, UMTS and LTE

MSISDN.(msisdn) is number "public knowledge" of the GSM or UMTS user as opposed to the IMSI number. It is this identifier, commonly called telephone number, which will be made to reach the subscriber. Only the HLR (Home Location Register) knows the correspondence between the MSISDN and IMSI number in the SIM card of the subscriber

PABX.: Private Automatic Branch Exchange -Expression Anglo-Saxon to describe a corporate **PBX,** known most commonly standard or private branch exchange. Telecommunications equipment automatically performing the switching of communications

UTRAN: UMTS Terrestrial Radio Access Network

Learning Activities

Activity - 1.First generations of mobile telephony networks and wireless

Introduction

Nowadays, the communications between mobile users are growing rapidly and represent a huge market. Among mobile users, we can mention those who have high mobility and changing geographic area and those using wireless access and remain still or move so little that they stay connected to the same network entry. Thus, three mobile generations have been and are distinguished by the transported communications. We distinguish three types:

- analog communication (first generation 1G)
- digital communication in the form of circuit, with two options: high mobility and reduced mobility (second generation 2G);
- multimedia applications as a package (third generation, 3G).
-

with improving the ubiquity and communication needs of more and more important it was necessary to increase the speed to more than 10 Mbit / s hence the birth of the fourth generation with the ability to connect to multiple networks simultaneously. The fifth generation of mobile telecommunication allows flow rates of several gigabits of data per second and up to 100 times faster than 4G 2020. Table A1.1.1 summarizes the different generations of mobile networks.

Generation	**WLANover**	**cellular Networks**
1st generation	CT0, CT1	NMT, RADIOCOM 2000, AMPS, TACS
2nd generation	CT2, DECT, PHS	GSM, D-AMPS, DCP, PCS1800 / 1900 IS95A / IS41 and IS136 / IS41
2nd generation and a half		GPRS , IS95B, EDGE
3rd generation		UMTS, W-CDMA, cdma2000, DECT,
3G and a half	Wi-Fi, WiMAX,	HSDPA, HSUP
4th generation	Multi-technology Wi-xx	HSDPA, UMB
4th generation and a half		LTE-B

Table A1. 1.1: Generations of mobile networks

The first mobile generation (1G)

During the first generation of wireless networks both standards have been developed:

- The CT0 (Cordless Telephone) was proposed in the 1970s to replace landlines. This is a simple analog system for domestic application. It uses FDMA transmission on a fixed frequency to 25 MHz and 40MHz. However, performance is modest and suffers from interference caused by electrical systems resulting in low transmission quality.
- The CT1 (Cordless Telephone Generation 1) is an analog system that was proposed by the 1980s and used in a some European country. The transmission is made with the FDMA of access technology at 900 MHz with a dynamic allocation of early radio communication channel. Note that each country has had to market a specific version which forced manufacturers to provide as many versions as there are countries. In addition, the CT1 does not allow wireless devices to communicate with stations of bases from other manufacturers and suffers from significant limitations on roaming and handover.
-

The first generation cellular networks were the first to allow a mobile user to use a continuously telephone anywhere in the service area of an operator.

The second mobile generation (2G)

The second generation wireless network

- The CT2 (Cordless Telephone Generation 2) standard provides wireless telephony on public roads regardless the manufacturer of the handset: Telepoint, small PBX. However, the CT2 does not ensure the handover resulting in reduced mobility. On the other hand, the roaming is manual manner. It is necessary that the user configures the handset when roaming. The CT2 provides telephone services and possible transmission of data and services for pedestrians.
- The DECT (Digital Enhanced Cordless Telecommunications) and PHS (Personal Handyphone System) provide radio coverage for use in residential (home base station) , office (wireless PBX) and on the street (public base station). The DECT standard developed by ETSI is a radio access standard operating in a frequency band between 1880 MHz and 1900 MHz. DECT uses the same technology that the cellular radio standards: digitally encoded information, cutting the coverage area in cells, TDMA technology. DECT uses a constant frequency hopping system and search for the best transmission which makes the system insensitive to interference. The DECT standard enables dynamic allocation of frequencies to users and enables the sharing between multiple operators. It is therefore not necessary to assign frequencies exclusively to operators. The frequencies are allocated to operators of public network non-exclusive basis as and when requested and without limiting the number of operators.
- The PHS is a wireless system offering a public access, both for domestic use professional, both inside and outside, with a handheld computer at very low cost. The PHS system is introduced commercially in Japan in 1995 as a public access system. Additional features are added quickly, as the implementation of wireless local loops, transmission of data at speeds that can be termed significant (32 or 64 Kbit / s) and homelessness, or roaming.

The technical complexity to access the service is quite low. The system perform handover, the user should always be within a cell and stay there.

The second generation of cellular networks

The second generation (2G) cellular networks differs from the first generation because it is Digital unlike the first generation was analog. In the early 1990s, several digital technologies have been proposed worldwide:

- GSM (TDMA-based), standard originated in Europe but used worldwide;
- iDEN (TDMA-based), proprietary network in the USA and Canada;
- cdmaOne (CDMA-based), used in the USA and parts of Asia
- PDC (TDMA-based), used exclusively in Japan;
- PCS, used in the USA consists of:
- PCS1800 / 1900 (or iS-95) based on CDMA technology
- GSM 900 that uses the TDMA radio technology
- D-AMPS(or IS-136) that uses TDMA

Digital cellular systems of second generation promote the development of a portable terminal with an acceptable autonomy.

GSM Global System for Mobile communications)

the GSM standard was created in 1982, at a meeting of the Special Mobile Group, later renamed the Global System for Mobile communications. Originally, the standard only used a radio frequency band around 900 MHz. It was extended to two other bands around 1800 and 1900 under the 1800 DCS names and DCS 1900 (standard mostly used in the United States).

Most GSM networks use the 900 MHz band or 1800 MHz . Some countries (Canada and USA) are using the frequencies 850MHz and 1900 MHz frequencies 400 and 450 MHz are rarely used, particularly Scandinavian, because these frequencies were used for 1G networks. The 900 MHz band uses a bottom-frequency between 890-915 MHz and 935-960 MHz for the downlink. These 25 MHz bands are subdivided into 124 channels, spaced 200 kHz. TDMA is used to allow 8 channels of voice transmission channel (carrier).

Security is ensured on network usage and conversations. GSM includes some security systems

- Against:Using a false identity
- Monitoring communications on a channel
- Monitoring positioning devices

This is possible thanks to the use of a secret key stored in the SIM card and is checked every call, and an encryption algorithm at the signaling .

Architecture and operation of the GSM

a GSM device (Mobile System - MS) is the combination of a terminal (phone) and a security module (SIM card, provided by the network operator). When a device connects to a network, the MS is sent to the HLR (Home Location Register). The HLR provides a temporary identity to the device to connect to the network. In roaming (roaming), the MS is relayed to the original HLR, which agrees with the current invoicing network to give the temporary identity.1.1.1.

Figure .1.1.1 level, it should be noted that the OSS (Operation Support SubSystem) is made by the NSS (Network and Switching Subsystem) and BSS (Base Station Subsystem).

a) The radio subsystem (BSS base station subsystem): It consists of:

- The BTS which makes dialogue with the Mobile Air interface (also called radio interface or Um interface). It controls the physical layer of the radio interface,

- Measurements on the uplink for the handover decision algorithm, makes mobile access application detections and handover access messages.
- The base station controller (BSC) that provides the control of one or more BTSs. Most of the smart features of BSS are located at its level, including radio resource management functions such as the allocation of cannaux, managing configuration cannaux, and treatment measures and intra BSC handover decision.

b) The network subsystem NSS (Network and Switching Subsystem) primarily provides switching and routing functions and provides access to the public network. It Gert functions of mobility management, security and confidentiality which are implanted in the GSM standard: it Constitute MSC, HLR, VLR, and AuC (Authentication Center) which stores a secret key for each subscriber. This key is used to authenticate requests for services and for encrypting communications. Note that a AuC is typically associated with each HLR.

c) The operational subsystem OSS (Operating Sub-System) ensures the management and supervision of the network. This function whose implementation is left with more freedom in the GSM standard call.

d) The call is transmitted by radio to the nearest base station (BTS) of the network, traveling from cell cell. The cell size depends on the environment. GSM 900 MHz, the cell size varies from 300 m radius in an urban environment, 30 km in open terrain. 1800 MHz GSM cells have, for their part, within 100 meters to 4 km. Once passed by the base stations, the call is relayed to a multiplexer (BSC). Once it gets to multiplexer, the call is then routed to its destination via the wired network. Obviously, if the call is to another mobile it will emerge from the wired network to run again in the air.

Table A.1.1.3 below is a comparison of different service standards and offers telephony systems first and second generation

	CT0 / CT1	analog Cellular	CT2	GSM	NCP DCS1800	DECT
Use	Domestic cordless PBX	Mobile	pedestrian Mobile without wireless PBX	Mobile	Mobile	PBX
Wireless	analog	analog	Digital	Digital	Digital	Digital
frequency band MHz	16/47 26/41 9000	200			400 900 900 900 1800 1900 1 800	
access mode	FDMA	FDMA	FDMA	TDMA		TDMA
Number of channels per tag	8/15/40	24	40			72144144
transmitter range	200 to 300 m	35 km	200 to 300 m	35 km	7 km	200 to 300m
transmission data	Not	Limited	No	Yes	Yes	Yes
Privacy	No	No		Yes	Yes	Yes
Roaming	No	Yes	manual		Yes	Manuel
Hand Over	No	Yes	No		Yes	Yes
Incoming Call		Yes	manual		Yes	Manuel
Call Outbound	Yes	Yes	Yes	Yes	Yes	Yes

Table A.1.1.3: comparative table of different systems

Conclusion

Although the cellular and wireless systems have evolved in order to meet user needs, current systems do not offer all the services expected by them. Note the lack of compatibility between the technologies discussed in this section. It is difficult to connect a DECT terminal to the GSM network market. Furthermore, a second radical change in telecommunications must be integrated into the mobile It is the explosion of traffic and Internet networks. Added to this is the rapid development of multimedia services. This development involves spectral resource needs as it may reach the limits of GSM. This development therefore calls for a new generation of systems for higher flows that will moreover a better allocation of spectrums. Therefore, new and more universal systems that integrate all these constraints be developed. Therefore we need new standards, so-called second generation and a half (2.5G) and third generation that are the subject of the following activities.

Evaluation

Before you attempt the questions read the notes above to familiarize yourself with definitions and network architectures that have been developed there. Furthermore, the learner will see the suggested readings for complete documentation.

Part Multiple Choice Questions (MCQ)

1. 2G is called. . . (1 point)

   a. The gsm

   b. The gprs

   c. Phs and pdc

2. WAP allows the GSM mobile? (2 points)

   a. To send a short message to another mobile

   b. by connecting to the internet thanks to a simplification of the XML syntax

   c. To increase the data transfer speed

   d. To sendvideo.

3. Portability allows? (2 points)

   a. Keep his number from one operator to another

   b. Keeping his mobile from one operator to another

   c. Keeping its service from one operator to another

   d. Keeping e-mail from one operator to another

4. The handover allows? (2 points)

   a. Keep a telephone call between two cell

   b. phones abroad

c. Keeping number

d. Increase flow.

5. A GSM terminal can perform a handover (1 point)

a. When in the course of communication

b. When in standby state

c. When it is off

d. several answers above

6. A GSM subscriber has a communication 20 minutes. What is the number of slots that is sent by the base station during communication? (3 points)

a. 2080000

b. 2600000

c. 260000

d. 208000

7. Can a GSM cell phone that works in the 1800MHz band it can work in the US.? (2 points)

a. yes

b. yes, provided you have a special subscription

8. What is the maximum bit rate between a mobile phone (MS) and a base station (BTS)? (2 points)

a. 33.875 kbit / s

b. to 200 kbit / s

c. 14.4 kbit / s

Part B: Questions

1. What are the differences between IMSI and MSISDN in a GSM network? (2 points)
2. What are the differences between HLR and VLR? (1 point)
3. During a cell change your telephone communication is interrupted while others already present in the new cell pursue their communication. What can be the reason of that? (2 points)
4. Q4. List the elements that constitute the radio subsystem BSS, NSS network subsystem and the operational subsystem OSS. (3 points)

5. Q5. Describe the role of each of the elements that constitute the BSS and the NSS. (5 points)

6. Q6. Illustrate GSM architecture indicating the BSS, NSS, and the OSS. (5 points)

7. Q7. Based on 3 criteria define and comparison of GSM, DECT and CT2. (3 points)

8. Q8. Why is portability of subscriber number is it possible in the GSM network? How is it done technically by the new operator. (5 points)

9. What is the function of the GMSC (Gateway MSC) in the GSM network (2 points)

Feedback

1. The answer is 260 000

2. Communication failure causes are many, include:

    a. mobile in a gray area ;

    b. low battery;

    c. moving speed of the mobile too important;

    d. movable range limit of a cell and overcapacity in the cell that would have given the position of the mobile, the support

3. For the choice of criteria the learner can draw from Table A.1.1.3 shows that the different systems.

4. Indeed, the network knows the IMSI and sends a symbiotic relationship between the MSISDN and IMSI. Either a fixed position that the MSISDN numbers (+221 77 xxx xx xx), the call is routed through the fixed telephone network to the switch from the nearest mobile network (MSC) that will bridge between the two networks (GMSC , Gateway MSC). The GMSC interrogates the HLR to know the location of the call. The HLR replaces the MSISDN IMSI (N□ attributed to locate the called party) and interrogates the VLR base which then assigns a MSRN (Mobile Station Roaming Number) number for call routing, this number consists of the country code VLR, the identifier of the VLR and the subscriber N□). The GMSC then establishes the call to the VMSC (Visited MSC). Finally, the VMSC establishes the call to the mobile using the temporary identity (TMSI)1.2.

Activity 2 - Evolution of mobile systems of second generation and a half (2.5G)

Introduction

Although the GSM and the second and other systems generation change, they are not able to meet the future needs of users. Users want ubiquity with the same terminal, be it at home, office, street, train, car, etc. Therefore, a new universal system that includes all the standards already developed a necessity.

GPRS (Global Packet Radio System)

On a technical level, the GSM network data transmission is simple because just dial the site number where the transfer will take place. The GSM network routes the call in question the interconnection circuit IWF (Inter Working Function). This completes the transfer to the remote terminal. The IWF operates in effect as a gateway. Modems with a battery as remote access servers of Internet service providers, the IWF performs translations between all GSM protocols and protocols used by different types of wired networks: PSTN, ISDN, X25 or other (see diagram). The data can be sent over the GSM network in transparent mode or non-transparent mode. In transparent mode, a connection is established without error correction and data is sent asynchronously. Data transmission takes place after a brief delay (latency). In non-transparent mode, the connection is established between the transmitter and receiver with error correction. The connection between the terminal and the GSM network uses the RLP (Radio Link Protocol) error correction. The IWF then establishes a connection with the remote modem using the V42 protocol. This second embodiment has two advantages, an increase in the data rate of approximately 20% and better management of calls through the GSM network.

GPRS is a packet switching technique which the door speed to 19.8 kbit / s / Time Slot. The standard, which is based on the fact that only the useful packets are transmitted, provides opportunities such as sharing resources among multiple users through an appropriate bandwidth allocation. Through coupling several time slots on the same radio channel, it will be possible to reach 156.4 Kbit / s rate for each channel. The theoretical speeds of 171.2 Kbps per mobile, nearly 18 times those of GSM network, enable mobile phones and PDAs equipped with communication systems, an almost instant connection and mostly permanent internet.

Currently, voice communication requires a single channel for transmission and reception. To transmit data, multiple channels are mobilized, thus increasing the rates. According to the technical specifications defined by ETSI (European Telecommunications Standards Institute), GPRS uses 8-channel (time slot) simultaneously to achieve the promised speed transmission. Only this speed is very theoretical. First, the first phones can manage only 4 channels, in particular for reasons of autonomy. The use of each channel requires almost as much energy as conventional GSM communication. Four channels simultaneously used therefore consume 4 times and 8.8 times.It is neccesary to say, in these conditions, the lifetime of a battery loses all chance of exceeding an hour or half an hour in communication . Each base station , which serves as a relay for communication has a fixed number of channels to be shared among users. The higher the number, the less they have canals and flows are low. Some of these channels are also reserved for voice calls, even only on a relay, a GPRS user can see its transmission speed restrained, especially a voice call has priority.

The final limitation is the network structure . Unlike GSM, GPRS is based on a packet transmission technology, such as the TCP / IP protocol on which the Internet. A document is sent in small pieces, the data packets. It is only when all the information has been transmitted, the recipient can receive them. To avoid packet loss inherent in this type of network and reinforced by the character of wireless GPRS, error correction protocols were in place. But, they all slow transmission.speed. Coding Schemes called, they each correspond to an actual flow rate: CS1: 9.05 kbps, CS2 13.4 kbps, CS3: 15.6 kbps, CS4: 21.4 kbps. In practice, because of radio interference of any sort, network coverage issues, CS1 and CS2 are most often used. Thus in reception, the throughput of a mobile GPRS oscillate between 36 and 53 kbps, approximately. In transmission, one channel is available, and flow do not exceed 9 kbps or that of GSM. This is far from advertised speeds. Using a packet transmission protocol enables a constant connection to the network, much like cable or DSL for the Internet, and opens up a new billing method. The conventional voice communications will remain charged to the duration, and volume data calls. This is to say that you can actually stay always connected without paying anything as long as no information is transferred.

However, technology keeps a permanent connection between the mobile and the enterprise. Indeed, the use of applications such as remote access to databases or information system is facilitated. Moreover, operators are deploying priority services for professionals. Technically there are three types of GPRS phone grouped into class A, B and C.

- The terminal class “A” handle voice and data simultaneously and includes most of the proposed models. A mobile GPRS class A can simultaneously connect to GSM networks (IMSI-Attach) and GPRS (GPRS-Attach). The mobile user can then simultaneously have a GPRS service and a telephone call. GPRS is supported by the SGSN (Service GPRS Support Node) while the telephone communication is supported by the MSC. A GPRS mobile class must have at least two TS (time slots) in the uplink direction and two ITs in the downward direction. TS the extra amenities it can be allocated for GPRS traffic to improve transfer speed.
- Class Terminal “B” handle voice and data alternately. A mobile GPRS class B may register with a MSC / VLR and SGSN simultaneously in order to have both GSM and GPRS services. Mobile requires at least one IT in the uplink and the downlink in IT. Additional ITs can read i be allocated for GPRS traffic to improve transfer speed.
- The class mobile “C” should position their mobile or in GSM mode or GPRS mode. In GSM mode, it has access to all the features of an ordinary GSM terminal. In GPRS mode, it can initiate data sessions. A GPRS mobile class C has two possible behaviors:
- Mobile GPRS Class CC: It registers to the GSM network and acts as a GSM mobile that can only access and circuit switching services C.
- Mobile GPRS Class It s’ registers to the GPRS network allowing access to the GPRS service only.

A GPRS mobile class C requires at least one iT in the uplink and the downlink in it. Additional TS can be allocated to the mobile GPRS class CG for GPRS traffic to improve transfer speed.

Figure A.1.2.1 shows the architecture of a GPRS network where a terminal communicates with a BTS (base transceiver station) GSM, but unlike calls data circuit-switched voice that are connected to the network through a MSC (Mobile Switching Center), GPRS packets are identified by a PCU then sent to the SGSN (Serving GPRS Support Node).

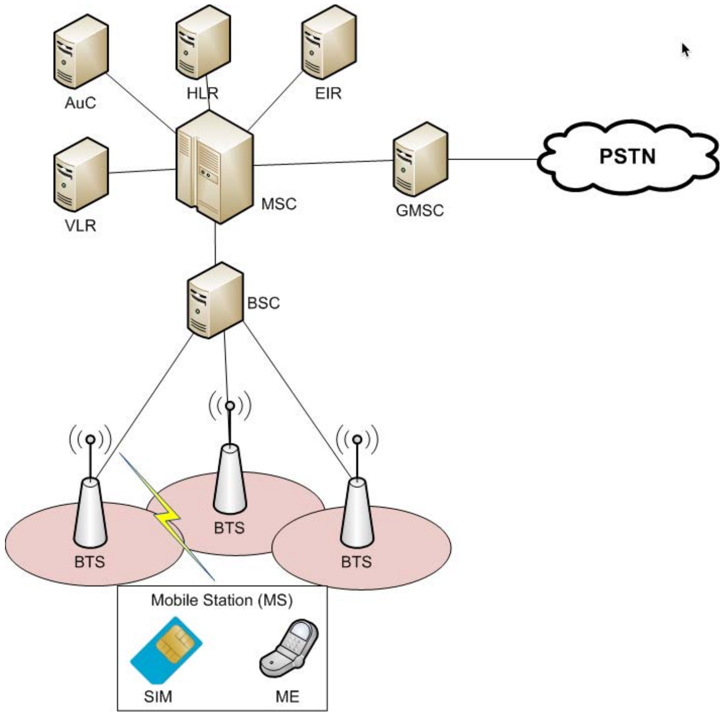


Figure A.1.2.1: Architecture of a GPRS network

Extracted from: https://upload.wikimedia.org/wikipedia/commons/d/df/Gsm_network_architecture.png

The SGSN is a node within the GSM infrastructure that sends and receives given with the mobile stations. It is also a router that manages the terminals present in a given area. The SGSN communicates with the GGSN (Gateway GPRS Support Node). This is the system which ensures the connections with other networks such as the Internet, a GPRS network can use multiple SGSN but requires only one GGSN to provide a connection to an external network.

The SGSN and GGSN are functional entities. They are separated in principle but in practice they can be combined in the same equipment. Each function has a fixed IP address. backbone called the assembly constituted by the GGSN, SGSN, IP routers and connections between equipment.

When the GPRS terminal sends data packets, they pass through the SGSN towards the GGSN. This converts to transmit through the desired network which can be either IP or X.25 networks. IP packets sent from the Internet and addressed to the GPRS terminal are received by the GGSN, the SGSN transmitted and routed to the terminal. To transit the IP or X.25 packet, the SGSN and the GGSN encapsulate using a specialized protocol, GPRS Tunnel Protocol, which is above the standard TCP / IP protocols.

Note that GPRS is itself likely to evolve towards EDGE (Enhanced data rates for GSM Evolution). The latter offers more speed (in practice 100 kbit / s) and requires a technical change less than for UMTS (It is described as such technology 2.75 billion)

EDGE technology (Enhanced Data Rate for GSM Evolution)

This is an intermediate technology between GSM and UMTS available since 2003. It provides quick access to the Internet at a speed of 200 Kbit / s for stationary users. It offers performance comparable to that of UMTS, but in the frequency band of GSM networks and with their TDMA technology. Edge was standardized at European level (Etsi / 3GPP) and internationally (ITU). Unlike UMTS, its use requires no special license. The Edge technology works on the band 800 and 1900 MHz 900.1800. Therefore there is no disruption of existing networks. The infrastructure required for packet transmission has already been put in place during the transition to GPRS.

The standard uses new coding schemes carry a new modulation technique called 8 PSK (8 Phase Shift Keying), which allows it to significantly increase its flow. This modulation allows the transfer of 3 bits per pulse, where the GPRS can not manage that (GSMK modulation). Edge technology, however, can also make the GSMK in case of failure, because the protocol is able to dynamically adapt the modulation and coding schemes. Edge has five additional patterns to increase the rate per channel up to nearly 60 Kbit / s, a theoretical maximum throughput of 473.6 kbit / s (160 for GPRS), voluntarily capped at 384 kbit / s ITU in order to integrate the IMT-2000 family of 3G standards.

Conclusion

The generation networks 2,5 are often characterized , as is the case in GPRS, by a double core network , a core network for carrying telephone and a core network for carrying data in packets . However, the GPRS provides a limited throughput which gives access to few uses . To overcome the limitations of GPRS, an evolution of GPRS called EDGE has been proposed and which straddles between GSM and UMTS. The EDGE has the advantage of using the infrastructure already deployed 2G unlike UMTS or 4G LTE networks.

Evaluation

The reading of the notes above and mastering of all the definitions and network architectures that have been developed there . Furthermore, the learner will necessarily consult the suggested readings for complete documentation.

Part A: Multiple Choice Questions

1. What is the other name for 2. 5G . . . (1 point)

    a. GSM

    b. GPRS

    c. THE EDGE

    d. UMTS

2. GPRS increases the rate of data transfer using : (1 point) using a new modulation

   a. Adapting protection system features of the radio channel

   b. by sending more bits per time slot

3. GPRS uses which technique : (1 point)

   a. packet communication

   b. communications circuits

   c .Internet communications

4. How many time slots can be used in GPRS ? (1 point)

   a. 1 to 8

   b. 4

   c. All free slot

5. The extension EDGE uses a new modulation name it ? (1 point)

   a. phase

   b. frequency

   c. amplitude

6. EDGE is considered by some traders as a telecommunications system name it ? (1 point)

   a. third generation

   b. Second generation

   c. second generation and a half

   d. GSM replacement

PART B

1. The GPRS network involves updating the software of the GSM network basics. Name it? (1 point)

2. GPRS involves the introduction of new equipment dedicated packet network to the existing GSM network. What are these elements and describe the role of each for access to data networks. (5 points)

3. Try to find through the readings and resources provided and the Internet for information on the two software systems used over GPRS . What is the difference between both ? (5 points)

4. What are the signs used at the GPRS network elements. (3 points)

Solution

1. Q2. The new equipment to be introduced are : PCU (Packet Controller Unit) , SGSN (Serving GPRS Support Node) , SGSN (Serving GPRS Support Node) , RGPRS (Register GPRS).

Activity 1.3 - The technologies of the third generation to fourth generation mobile

1. Introduction

The third generation (3G) allows you to enjoy much higher data rates than GPRS and EDGE . Thus , 3G offers a range of telecommunications services to fixed and mobile users, located in a variety of environments around the frequency of 2 GHz . It is designed for the exchange of data and multimedia content at broadband packet . There exist different implementations in the world: W -CDMA (Wideband CDMA) called UMTS in Europe and Japan, CDMA 2000 in the United States , Southeast Asia and Japan.

2. UMTS (Universal Mobile Telecommunication System)

It is well known that UMTS is a wireless technology based on the CDMA (Code Division Multiple Access), a highly complex access method that was used on the networks of the second generation in America and Asia .The layman may wonder about the interest to rely on this unknown technology, particularly in Europe, rather than on the technology of GSM, TDMA ... But only the evolution of 3G CDMA [ie the Wideband CDMA] is able to meet the bandwidth requirements of the new generation of mobile telephony. CDMA capabilities are more powerful effect in relation to other radio networks generations (see chart). The first generation, that by the free Radiocom 2000 service 1980, allocated a frequency for a user: the FDMA (Frequency Division Multiple Access). TDMA (T for Time Division Multiple Access) technology used by the current GSM adds time as a variable, allowing multiple users to share the same frequency sequentially, which already offers a much better use of the radio spectrum. CDMA goes one step further by allowing all users to transmit simultaneously on the same frequency. To recognize each of them, a code is assigned to each communication facility coding that is recognized by the UMTS base stations. The radio resources are then optimized to minimize the interference level. Obviously, this increase in transmission capacity has another side: the complexity. UMTS is indeed a clever compromise between capacity and coverage between capacity and radio performance, for each cell.

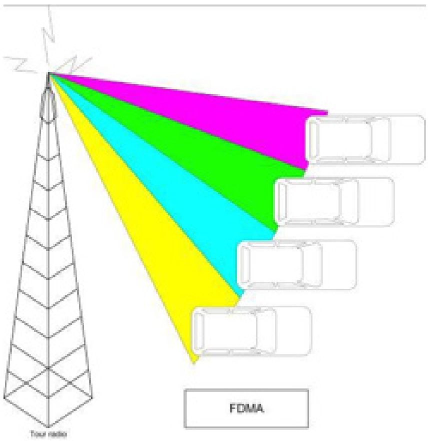


Figure A.1.3.1 :FDMA , TDMA and CDMA access techniques

Extracted from: http://lexique.reseaux.free.fr/Fichiers/Lexique%20de%20Termes%20et%20 Acronymes%20Reseaux%20&%20Telecom.pdf

The hierarchy of UMTS cells

UMTS uses an adjacent frequency range of 2 GHz. The channels division is made, then, per 4 5 MHz. Such bandwidth enables a frequency spectrum even wider than the noise can be reduced and isolated. The UMTS Forum therefore recommends the allocation to each UMTS operator of 35 MHz (or 2 * 15 + 5) to meet the needs until 2005. On 30 MHz communications will be provided for one direction of transmission, while 5 MHz we both transmission directions for the same frequency. In addition, a recovery in GSM bands could be considered (GSM: around 900 MHz and 1800 MHz). First, it will ensure compatibility with third generation terminals and second-generation cells. Therefore the frequency bands must be in multiples of 20 KHz (GSM frequency band) and flow rates will be derived from a common clock to that of GSM (13 or 26 MHz).

The UMTS coverage is divided into a plurality of variable-sized cells. Each cell presents itself as a function of population density used and the speed of mobility. So we have three types of cells:

- The macro- cell (coverage radius of 15 km), allow speeds of around 144 kbit / s during a displacement of the order of 500 km / h (High Speed Train , etc.).
- The microcells (500m) allow data rates of the order of 384 kbit / s during a displacement of the order of 120 km / h (vehicle , public transport , etc.).
- The pico- cells (100m) allow data rates of around 2 Mbit / s during a displacement of around 10 km / h (walking, indoor travel, etc.) .

Figure A1.3.2 shows the architecture of a 3G system. The idea developed by the architects of the 3G network is left of the core network untouchable existing GSM network and add features that methods manages the data. UMTS will rely on GSM for global coverage , with the aim that in any geographical point UMTS is accessible directly either broadband or degraded so when the GSM will take over. This hedging method therefore require the development of multimode

GSM / UMTS terminals to ensure continuity of service. For higher throughput and better use of the frequency spectra , ETSI decided to use a communications protocol called UTRA . The UTRA is based on the CDMA technology that allows the same frequency to accommodate multiple users through modulation spread spectrum .

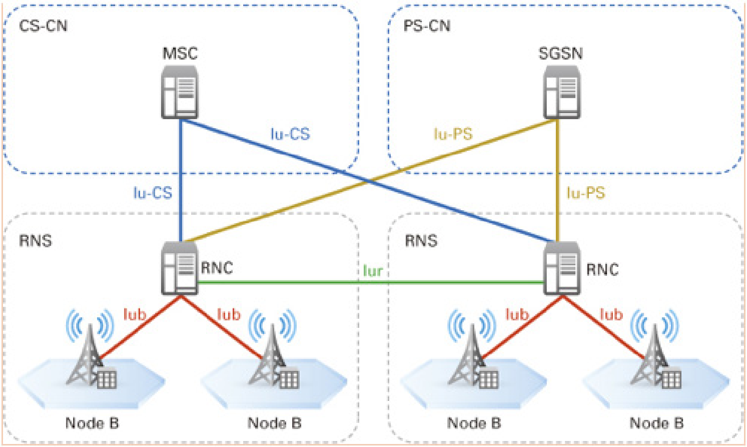


Figure A.1.3.2 : Architecture of a 3G syste

Extracted from: : Computer Networking A Top Down Approach, Kurose et Ross, 6th Edition,PEARSON, 2013.

SGSN (Serving GPRS Support Node) is a node within the infrastructure that sends and receives given with the mobile stations. It is also a router that manages the terminals present in a given area. The SGSN communicates with the GGSN (Gateway GPRS Support Node). This is the system that provides connections to other networks like the Internet. The SGSN interacts with the MSC is located in its vicinity.

Note that the HSPA (High Speed Packet Access) shown at the radio interface in a generic term adopted by the UMTS for naming enhancements of UMTS radio interface. HSPA mean enhancements to both the downward flow (HSDPA) and upflow (HSUPA). As part of the evolution of GSM to 3G, HSPA enables faster data transfer, to enhance spectral efficiency and increase the capacity of operators of systems. Regarding users, HSPA provides access to a world of mobile high-speed multimedia services.

UTRAN access network (UMTS Terrestrial Radio Access Network

The UTRAN access network has several features. Its main function is to transfer data generated by the user. It is a gateway between the user equipment and network core through different (Figure A.1.3.2)

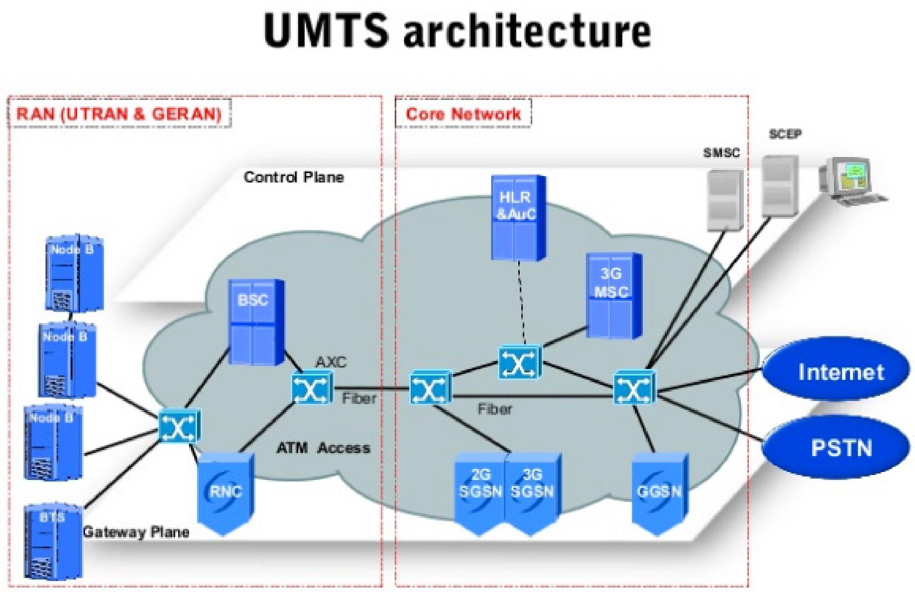


Figure A1.3.2 : Architecture of UMTS

Source : http://www.slideshare.net/gprsiva/04-umts-traffic-managementnew

The primary role of the RNC (Radio Network Controller) is to route communications between the NodeB and heart network of UMTS. The RNC works at Layer 2 and Layer 3 of the OSI model (power control, code allocation) . The RNC is the access point for all the core network services .

However, the UTRAN access network is responsible for other matters :

- Security: It provides privacy and protection of information exchanged by the radio interface using algorithms encryption and integrity.
- Mobility: An estimate of the geographical position is possible with the UTRAN access network.
- Radio Resource Management: The access network is responsible for allocating and maintaining radio resources for communication.
- Synchronization: It is also in charge of maintaining the reference time base of mobile to transmit and receive information.

The UTRAN access network consists of several elements : one or more base stations (called Node B) , radio controllers RNC (Radio Network Controller) and communication interfaces between the different elements of the UMTS network . Note that the primary role of Node B is to ensure the functions of receiving and radio transmission to one or more cells of the UMTS access network with a user equipment. two types of nodeB : nodeB with sector antennas and node B with omnidirectional antenna .

We have four communication interfaces :

- Uu : it is the communication interface via CDMA technology between user equipment and the UTRAN access network.
- this is the interface between the UTRAN access network and the network of UMTS heart . This interface allows the RNC radio controller to communicate with the SGSN
- this is the interface that allows two controllers to communicate RNC radio
- this is the interface that enables communication between a NodeB and RNC radio controller.

Generation

It is often considered that the 3.5G line with high data rates, that is to say more than 1 Mbit / s. This value is obtained by HSDPA in the downlink direction and his successor in the HSUPA uplink . We detail these two technologies in this section. Note that to enter the fourth generation, it is necessary that the flows exceed the ten megabits per second.

HSDPA

HSDPA (High-Speed Downlink Packet Access) is a protocol for mobile telephony sometimes called 3G +. This protocol provides performance about ten times the 3G (UMTS R5). It is essentially a software upgrade that allows this increase in rates. HSDPA has a downlink ⍰ the network to the terminal ⍰ packet strong increase compared to UMTS. HSDPA is part of the family HSPA (High-Speed Protocol Access). The existing deployment offers speeds of 1.8 Mbit / s, 3.6 Mbit / s, 7.2 Mbit / s and 14.4 Mbit / s on the downlink and even much more with the advanced version, which reaches 42 Mbit / s. Another even more important aspect is the overall bandwidth, allowing many clients to connect simultaneously. HSDPA is a relatively simple upgrade to UMTS, and that's why we class in the 3.5G.

Transmission occurs by "trunked" (High Speed Downlink Shared Channels), each to manage up to fifteen transmission codes. Depending on the needs of connected users and the ability of their terminal, they will receive one or more codes in the connection and can switch from one channel to another 2 milliseconds (10 to 20 ms for UMTS). HSDPA uses in addition an additional frequency modulation technique compared to UMTS (the latter merely the Quadrature Phase Shift Keying (QPSK)). HSDPA adds the 16-quadrature amplitude modulation (16QAM). 16-QAM doubles transfer capacity compared to QPSK, but in return requires very good radio conditions. To manage this type of constraint, HSDPA is subject to immediate adaptation of transmission parameters mechanisms. If environmental degradation, resources (codes, time intervals, etc.) will be reallocated to better and more or less of the bandwidth will be used for error correction data. The optimal exploitation of all these techniques (using fifteen codes with double QPSK / 16-QAM, error data transfer without) offers the theoretical maximum rate of 14.4 Mbit / s.

HSUPA

HSUPA (high-speed uplink packet access) is an evolution of UMTS that changes the emission flow (in the sense terminal -> Network) . This development is a challenge for handset manufacturers since it results in significant energy consumption. Indeed, the flow could be up to 5.76 Mbit / s. The specification of the HSUPA is in the document 3GPP R6 (release 6). HSUPA uses an enhanced uplink channel called E -DCH (Enhanced Dedicated Channel) , which uses the same ingredients as HSDPA on the downlink channel , adapting the communication between the terminals and the NodeB to optimize the overall use of the channel.

After HSUPA , 3GPP has worked to further improvement to go

to the high flow: the HSOPA (High Speed OFDM Packet Access), which marks the beginning of the fourth generation mobile networks.

4G LTE (Long-Term Evolution)

It is based on an IP core network, the future 4G telephony system provides high-speed data access, enabling uninterrupted service transition between multiple radio access points. 4G network, convergence of multiple networks does not cause disruptive technology with the 3G (UMTS). 4G is characterized by an IP core network and the management of many radio access technologies.User can access of all data .

The 4G network provides significantly higher speeds: between 20Mb/s and 100 Mb / s in the long-range networks (UMTS) and up to 1 Gbit / s in local networks such as WiFi hot spots. These flows ensure the transmission of multimedia content increasingly rich, and will establish several parallel sessions (for example a high quality video conferencing session with real-time access to multimedia content.)

With the 4G network, users can access their data wherever they are: at home or in businesses (Bluetooth, UWB or WiFi UMTS) or even in public places equipped with hot spots . Switching from one network to another is transparent. Finally, flow rates (up to 100 Mb / s on the move, and 1 Gb / s in closed environments) provide access to many multimedia applications in parallel.

- 4G LTE has two major innovations compared to 3G networks: Evolved Packet Core (EPC): this is a core network "All IP" simplified and unifies the circuit switched network used by voice and packet-switched network used for data. It is a network in which all IPs in the sense that voice and data are carried in IP datagrams. Since the IP network operates in "Best-effort," the main role of the EPC is to manage resources to ensure high quality of service for applications that have time constraints and bandwidth. These transmission channels are extremely important because they are set based on the performance characteristics defined by the user or the operator. The EPC also separates the control channel and the data channel. Therefore, behind every successful LTE connection hides an EPC system to support user data traffic and control signaling.

- LTE Radio Access Network : LTE uses OFDM (orthogonal frequency division multiplexing) and each mobile can receive one or more slots with a duration of 0.5 ms in one or more transmission channels. By increasing the number of slots to be used on the same frequency or other frequencies, one node increases considerably its flow rate. The allocation of slots or their re- allocations between nodes can be made every millisecond . Another innovation of LTE is the possibility of using multiple antennas for transmission and multiple antennas for reception. This transmission technique is called MIMO (Multiple -Input , Multiple Output) . The maximum speed of an LTE user in the downlink is between 100 Mb / s and 50 Mb / s in the uplink direction when the frequency of 20 MHz of wireless spectrum is used .

Conclusion

The integration and compatibility between different networks corresponding to different standards (UMTS , WCDMA, cdma2000 , GSM, LTE , etc.) will allow roaming and interoperability. The user can move between third-generation and fourth generation networks seamlessly while maintaining service continuity , even if in some cases the quality will be affected because of the characteristics of a new radio environment.

Évaluation

Before being evaluated the learner is expected to read the notes above and master all the definitions and network architectures that have been developed there . Furthermore, the learner will have the suggested readings for complete documentation.

Questions:

1. Based on the three criteria define and compare TDMA techniques, FDMA , CDMA . (3 points)

2. Explain the technical reasons why 4G was introduced . (3 points)

3. Describe the functions of the UTRAN access layer (3 points)

4. On which layer of the OSI model does nodeB works ? (1 point)

5. What are the advantages of the use of OFDM and MIMO at the radio layer of LTE . (3 points)

6. What are the three platforms used by the EPC to connect the user to the mobile communications universe? (3 points)

7. What are the differences between LTE and advanced LTE? (4 points)

8. Illustrate applications of existing networks , and breaking innovation posed by 4G using their social and economic consequences . (5 points)

9. What are the main differences between UMTS and HSDPA ? (3 points)

Solutions

1. The learner can look through the resources the role of the 3 three elements of the EPC: MME (Mobility Management Entity) , SGW (Serving Gateway) , SGW (Packet Data Network Gateway)

2. The learner can access http://www.3gpp.org/DynaReport/36-series.htm where LTE and Advanced LTE standards are described.

3. The main differences with UMTS are the following functions:

Retransmissions much faster from the NodeB through the algorithm HARQ (Hybrid Automatic Repeat Request) .

Reordering in the NodeB much faster than UMTS through the SPF algorithm (Fast Packet Scheduling) .The type of Modulation and coding type is AMC (Adaptive Modulation and coding)

UNIT SUMMARY

Cellular networks of first generation were the first to allow a mobile user to use a continuously telephone anywhere in the operator of a service area. Subsequently, a second generation GSM network was launched. There was a lack of compatibility between the various second generation technologies. It is difficult to connect a DECT terminal to the GSM network. With the explosion of traffic, Internet networks, the rapid development of multimedia services, the GSM network quickly reached those limits. This development involves spectral resource requirements. Therefore there was a need to have new standards, so-called second generation and a half (2.5G) and third generation.

For a core network "all-IP", allow a convergence of all existing technologies, providing a quality service to all applications that have bandwidth and delay constraints .4G network is currently being applied in mobile networks.4G is characterized by an IP core network and the management of many radio access technologies.

Many specific applications utilize the capabilities of mobile systems to deliver sound, still and moving image data and telemedicine , reporting, tracking , monitoring , information and route guidance .

Unit Evaluation

1. Read the lecture notes associated with Unit 3
2. Read suggested readings and resources
3. Validate all learning activities Unit 3
4. Train regularly on the constituents of 3G and 4G network architectures as well as their roles.

Rating System.

Question 1: (4 points)

Question 2: (4 points)

Question 3: (4 points)

Question 4: (4 points)

Question 5: (4 points)

Evaluation

1. Give the general block diagram of a digital transmission chain GSM and briefly explain the role of each block.

2. Explain how GSM / GPRS works as a part of network to manage making calls and internet data transfer?

3. Illustrate the architecture of the 3G network and describe the role of the UTRAN access architecture and communication interfaces.

4. Give the advanced LTE developments with respect to LTE .

5. What is the relationship between 2G , 3G and 4G ?

Readings and Other Resources

Readings and other resources of this unit are at lectures and other course resources.

List of relevant readings :

Lecture 1

1. http://www.wirelesscommunication.nl/pdfandps/systems.pdf
2. http://www.artizanetworks.com/lte_resources/lte_tut_what_lteenb.html

Summary: These lecture notes deal with GSM networks and different technologies in several generation of networks.

Justification : This documents can assist acquire a general knowledge about the evolution of mobile networks from the first generation to the third generation . Reading this document allows to better understand the concepts discussed in Chapters 1 , 2 and 3 of this unit.

Lecture 2 : Ganz, A., Ganz, Z., & Wongthavarawat, K. (2003). Multimedia Wireless Networks: Technologies, Standards and QoS. Pearson Education.

Gibson, J. D. (Ed.). (2012). Mobile communications handbook. CRC press.

https://books.google.co.ke/books?id=Y-91Z3y-gokC&printsec=frontcover&dq=evolution+of+2+and+2.5+g+networks+pdf&hl=en&sa=X&ved=0ahUKEwiXhZC-4KbLAhXMfhoKHQNXBEkQ6AEIIzAA#v=onepage&q=evolution%20of%202%20and%202.5%20g%20networks%20pdf&f=false

Justification : The readings in chapter two allows the learner to know different wireless standards Reading this chapter provides insight into the reasons for the transition from 1st generation to 3rd generation or 4th generation mobile networks.

Lecture 3 Glossary of Terms and Acronyms Networks & Telecom

www.ijcta.com/documents/volumes/vol5issue5/ijcta2014050534.pdf

Summary: In this document there will be illustration on different generations of networks.The network summary of 1G,2G,3G,4G features are explained

Lecture 4 : LTE (Long Term Evolution)

http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf

Summary: In this document there will be an overview of 4G networks its architecture and a brief history .

Justification:By studying this document , the learner is better equipped to know in detail the LTE architecture as well as its operation. Reading this document allows to better understand the concepts presented at the 4 activity of this unit.

List of suggested resources :

Lecture 4: 3GPP R6 (release 6)

http://www.3gpp.org/specifications/releases/74-release-6

Accessed February 24, 2016

Abstract: This paper presents the technical operation of the radio interface HSUPA

Justification : In browsing this document , the learner is better equipped to know the HSUPA standard as what is described by the 3GPP group

REFERENCES

1. Gibson, J. D. (Ed.). (2012). Mobile communications handbook. CRC press
2. Ganz, A., Ganz, Z., & Wongthavarawat, K. (2003). Multimedia Wireless Networks: Technologies, Standards and QoS. Pearson Education..
3. http://lexique.reseaux.free.fr/Fichiers/Lexique%20de%20Termes%20et%20Acronymes%20Reseaux%20&%20Telecom.pdf
4. https://books.google.co.ke/books?id=Y-91Z3y-gokC&printsec=frontcover&dq=evolution+of+2+and+2.5+g+networks+pdf&hl=en&sa=X&ved=0ahUKEwiXhZC-4KbLAhXMfhoKHQNXBEkQ6AEIIzAA#v=onepage&q=evolution%20of%202%20and%202.5%20g%20networks%20pdf&f=false
5. www.ijcta.com/documents/volumes/vol5issue5/ijcta2014050534.pdf
6. http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf
7. http://www.3gpp.org/specifications/releases/74-release-6

Unit 4. Mobile and wireless security

Unit Introduction

The evolving trend of cellular devices devices has been subjected to high risks since they are always on and accessible.they provide means of communication and connectivity through different types of services that are offered by communication services.wireless networks and mobile network services always work together.All communication equipments are designed to provide access of information from one point to the other.A mobile or wireless network can connect to different types of devices and each communication will require a type of security authentication and security

Unit Objectives

Upon completion of this unit you should be able to:

- To analyze basic concepts of wireless network security
- To classify different types of attacks and threats that occur in mile and wireless computing
- To outline different methods of implementing wireless security
- to analyze methods used in securing information.

Key Terms

1. 3DES Triple Data Encryption Standard
2. AES Advanced Encryption Standard
3. BS Base Station
4. BSC Base Station Controller
5. ECP Encryption Control Protocol
6. EDGE Enhanced Data Rates for GSM Evolution
7. ECP Encryption Control Protocol
8. GPRS General Packet Radio Service
9. GPS Global Positioning System
10. MSA Mobile station authentication
11. RAND Random Number
12. GSM Global system for mobile

13. MS Mobile station
14. AuC Authentication Center
15. MSC Message switching Center
16. SRES Signed Response
17. BTS Base Transceiver station
18. SIM Subscriber identity module
19. VLR Visitor location register
20. HLR Home location register
21. EIR Equipment identity register
22. PSTN Public switch telephone network
23. ISDN integrated service digital network
24. TMSI Temporary Mobile Subscriber Identity
25. IMSI international mobile subscriber identity

Learning Activities

Activity 1.1 - Introduction to security

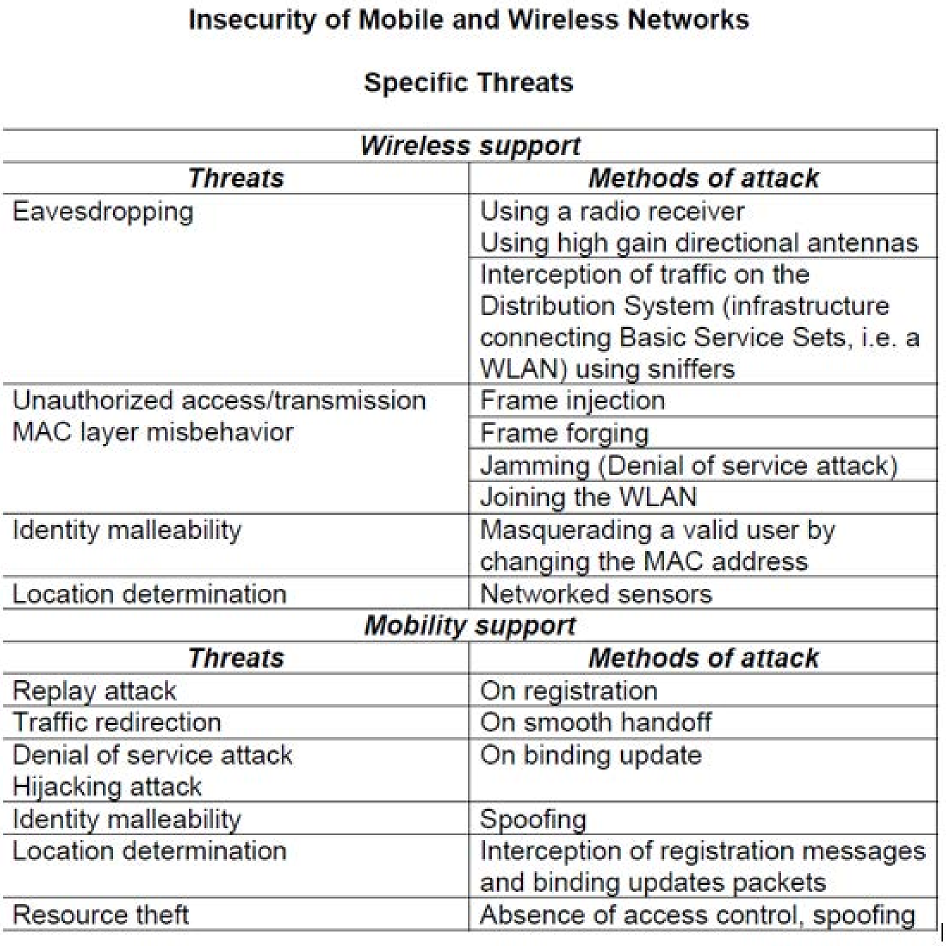
Introduction

All wireless and mobile communications have an increased risk rate of eavesdropping in transmission of data over different modes of communication.The security attempts tries to ensure that there is maximum levels of the CIA triad by improving confidentiality, integrity, and availability of computing systems' components.Depending on the wireless technology used different security measures and techniques are needed and they appear at different levels of communication .These three, and the communications among them, constitute the

basis of computer security vulnerabilities. In turn, those people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities. This chapter has identified four kinds of attacks on computing systems: interception, interruption, modification, and fabrication.

Activity Details

There are different types of security violations that can occur in a mobile and wireless computing as shown in the table below:



Insecurity of Mobile and Wireless Networks

Specific Threats

Wireless support	
Threats	***Methods of attack***
Eavesdropping	Using a radio receiver Using high gain directional antennas
	Interception of traffic on the Distribution System (infrastructure connecting Basic Service Sets, i.e. a WLAN) using sniffers
Unauthorized access/transmission MAC layer misbehavior	Frame injection
	Frame forging
	Jamming (Denial of service attack)
	Joining the WLAN
Identity malleability	Masquerading a valid user by changing the MAC address
Location determination	Networked sensors
Mobility support	
Threats	***Methods of attack***
Replay attack	On registration
Traffic redirection	On smooth handoff
Denial of service attack Hijacking attack	On binding update
Identity malleability	Spoofing
Location determination	Interception of registration messages and binding updates packets
Resource theft	Absence of access control, spoofing

Security Goals

The term security appears in many ways in our day to day lives.A "security system" protects our house, warning the neighbors or the police if an unauthorized intruder tries to get in. "Financial security" involves a set of investments that are adequately funded; we hope the investments will grow in value over time so that we have enough money to survive later in life. And we speak of children's "physical security," hoping they are safe from potential harm. Just as each of these terms has a very specific meaning in the context of its use, so too does the phrase mobile and wireless computing security

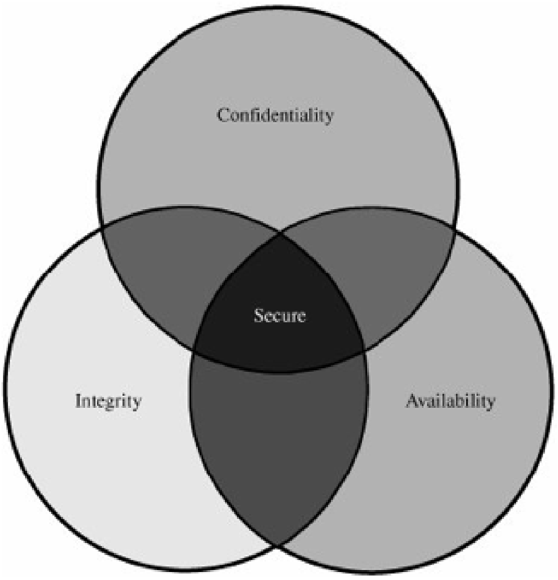
When we talk about mobile and wireless security, we mean that we are addressing three important aspects of any wifi, GSM, GPRS and different generations of mobile network system

THE THREE GOALS OF WIRELESS AND MOBILE SECURITY

confidentiality, integrity, and availability.

- Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy.
- Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.
- Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.

Security in computing addresses these three goals. One of the challenges in building a secure system is finding the right balance among the goals, which often conflict. For example, it is easy to preserve a particular object's confidentiality in a secure system simply by preventing everyone from reading that object. However, this system is not secure, because it does not meet the requirement of availability for proper access. That is, there must be a balance between confidentiality and availability.



The relationship between confidentiality integrity and availability.

Confidentiality

confidentiality may seem to be a straightforward aspect in dealing with security issues.Only authorized people or systems can access protected data. However, ensuring confidentiality can be difficult. For example, who determines who to access a certain network in the system and by accessing the system which kind of data should be available for him.Data may have different priority by different users of the network user.Only authorized people or systems should be accessible at different intervals of time,otherwise the information should not be disclosed to other parties

Confidentiality is the security property we understand best because its meaning is narrower than the other two. We also understand confidentiality well because we can relate computing examples to those of preserving confidentiality in the real world.

Integrity

Integrity is much harder to pin down. As Welke and Mayfield [WEL 90, MAY 91, NCS91b] point out, integrity means different things in different contexts. When we survey the way some people use the term, we find several different meanings. if we say that we have preserved the integrity of an entire system of communication, we may mean that the item is:

- Precise
- Accurate
- Unmodified
- Modified only in acceptable ways
- Modified only by authorized people
- Modified only by authorized processes
- Consistent
- Internally consistent
- Meaningful and usable

Integrity can also mean two or more of these properties. Welke and Mayfield recognize three particular aspects of integrity authorized actions, separation and protection of resources, and error detection and correction. Integrity can be enforced in much the same way as can confidentiality: by vigorous control of who or what can access which resources in what ways. Some forms of integrity are well represented in the real world, and those precise representations can be implemented in a computerized environment. But not all interpretations of integrity are well reflected by communication implementations.

Availability

Availability applies both to data and to services (that is, to information and to information processing), and it is similarly complex . As with the idea of confidentiality, different people expect availability to mean different things. For example, an object or service is thought to be available if

- It is present in a form that can be used.
- It has capacity enough to meet the service's needs.
- It is making clear progress, and, if in wait mode, it has a bounded waiting time.
- The service is completed in an acceptable period of time.
- The service is available to the intended system
- The service is available at the time that it is needed.

When the system is tested one of the greatest task is to have an imagination of what would happen if the system fails or malfunctions.This would and up to designing a system that can withstand any problem that is identified.There is also an need to analyze any other possible ways in which the system may malfunction and diminish the goals and the values of the system.

Vulnerabilities, Threats, Attacks, and Controls

A mobile-based system has three separate but valuable components: hardware, software, and data. Each of these assets offers value to different members of the community affected by the system. To analyze security, we can brainstorm about the ways in which the system or its information can experience some kind of loss or harm. For example, we can identify data whose format or contents should be protected in some way. We want our security system to make sure that no data are disclosed to unauthorized parties. Neither do we want the data to be modified in illegitimate ways. At the same time, we must ensure that legitimate users have access to the data. In this way, we can identify weaknesses in the system.

A vulnerability is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

There are many threats to a mobile system, including human-initiated natural-initiated and computer-initiated ones. We have all experienced the results of inadvertent human errors, hardware design flaws, and software failures. But natural disasters are threats, too; they can bring a system down when the service center room is flooded or the data center collapses from an earthquake, for example.

A human who exploits a vulnerability perpetrates an attack on the system. An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function. Unfortunately, we have seen this type of attack frequently, as denial-of-service attacks flood servers with more messages than they can handle.

this problem can be addressed by the use a control as a protective measure.

The control can be an action device, procedure, or technique that removes or reduces a vulnerability.In general, we can describe the relationship among threats, controls, and vulnerabilities in this way:

A threat is blocked by control of a vulnerability.

There must be a consideration of up to what extent the system security should be enhanced so that to get the maximum control and reduce threats as much as possible .threats can be categorized in four kinds:

- Interception
- Interruption
- Modification
- Fabrication.
- An interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illegal tapping of a communication line and getting the information and data from the network . Although tapping may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.
- In an interruption, an asset of the system becomes lost, unavailable, or unusable. A good example is a malicious destruction of a communication channel and deleting, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular file.
- An unauthorized party may not only access the system he may tamper with the information or data that is available by changing the contents, the threat is a modification. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted through a wireless media. It is even possible to modify hardware making it malfunction or perform different tasks against the ones that they were intended for . Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.
- Finally, an unauthorized party might create a fabrication of counterfeit objects on a wireless system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

These four classes of threats interception, interruption, modification, and fabrication describe the kinds of problems we might encounter. In the next section, we look more closely at a system's vulnerabilities and how we can use them to set security goals.

What are the methods opportunity and motives of the attack?

A malicious attacker must have three things:

- Method: the skills, knowledge, tools, and other things with which to be able to pull off the attack
- Opportunity: the time and access to accomplish the attack
- Motive: a reason to want to perform this attack against this system

Conclusion

Security attempts to ensure the confidentiality, integrity, and availability of communication systems' components. Three principal pieces of a computing system are subject to attacks: hardware, software, and data. These three, and the communications among them, constitute the basis of computer security vulnerabilities. In turn, those people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities. This chapter has identified four kinds of attacks on computing systems: interception, interruption, modification, and fabrication

Assessment

1. Distinguish among vulnerability, threat, and control.

2. Theft usually results in some kind of harm. For example, if someone steals your car, you may suffer financial loss, inconvenience (by losing your mode of transportation), and emotional upset (because of invasion of your personal property and space). List three kinds of harm a company might experience from theft of computer equipment.

3. List at least three kinds of harm a company could experience from electronic espionage or unauthorized viewing of confidential company materials.

4. List at least three kinds of damage a company could suffer when the integrity of a program or company data is compromised.

5. Describe two examples of vulnerabilities in automobiles for which auto manufacturers have instituted controls. Tell why you think these controls are effective, somewhat effective, or ineffective.

6. One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?

Activity 1.2 -Basic Cryptography

Introduction

Cryptography or secret writing is the strongest tool for controlling against many kinds of security threats. Well-disguised data cannot be accessed, modified, or fabricated easily. Cryptography is rooted in higher mathematics: group and field theory, computational complexity, and even real analysis,not to mention probability and statistics. Fortunately, it is not necessary to understand the underlying mathematics to be able to use cryptography.

Activity Details

Consider the steps involved in transmitting a message, S, to a recipient, R. If S entrusts the message to T, who then delivers it to R, T then becomes the transmission medium. If an outsider, O, wants to access the message (to read, change, or even destroy it), the interceptor or the intruder O . Any time after S transmits it via T, the message is vulnerable to exploitation, and O might try to access the message in any of the following ways:

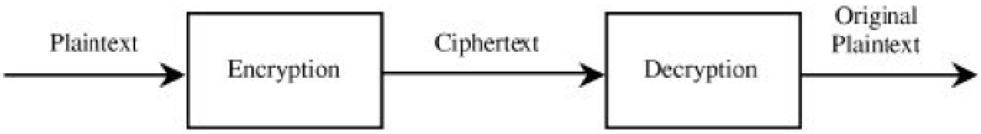
Block it, by preventing its reaching R, thereby affecting the availability of the message,

Intercept it, by reading or listening to the message, thereby affecting the confidentiality of the message.

Modify it, by seizing the message and changing it in some way, affecting the message's integrity.

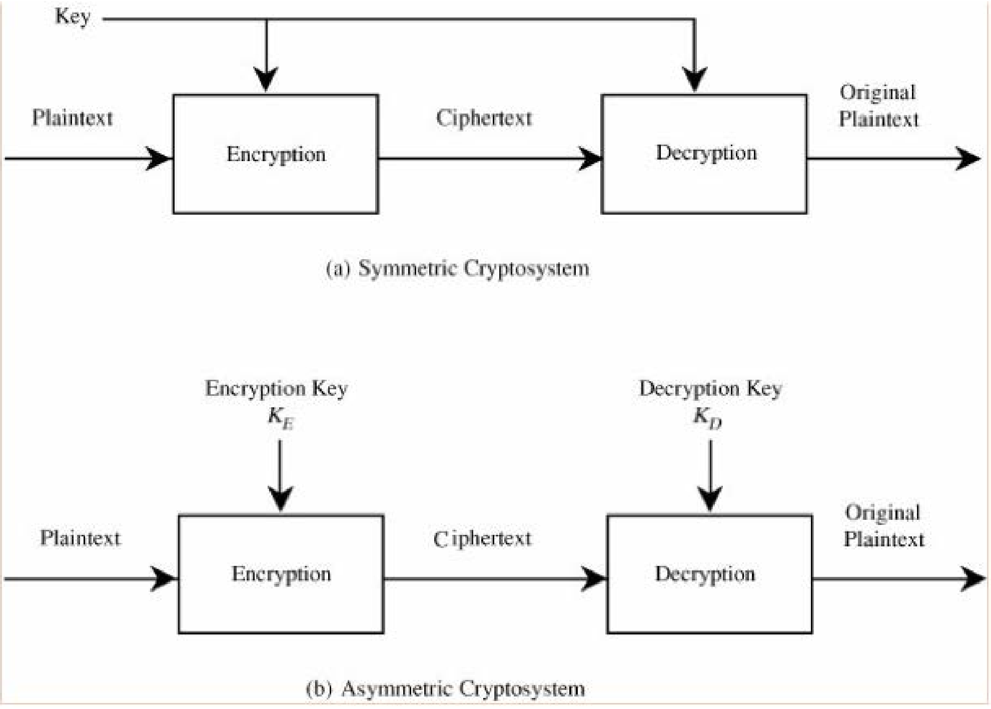
Fabricate an authentic-looking message, arranging for it to be delivered as if it came from S, thereby also affecting the integrity of the message.

The original form of a message is known as plaintext, and the encrypted form is called ciphertext. This relationship is shown in below. For convenience, we denote a plaintext message P as a sequence of individual characters P = <p1, p2, …, pn>. Similarly, ciphertext is written as C = <c1, c2, …, cm>. For instance, the plaintext message "my name is John" can be denoted as the message string <m,y, ,n,a,m,e,,i,s,,j,o,h,n,>. It can be transformed into ciphertext <c1, c2, …, c14>, and the encryption algorithm tells us how the transformation is done.



There are two types of cryptosystems which depend on the key uses.Asymmetric cryptosystem uses different keys for encryption and symmetric cryptosystem uses single key for both encryption and decryption.

A key gives us flexibility in using an encryption scheme. We can create different encryptions of one plaintext message just by changing the key. Moreover, using a key provides additional security. If the encryption algorithm should fall into the interceptor's hands, future messages can still be kept secret because the interceptor will not know the key value. An encryption scheme that does not require the use of a key is called a keyless cipher.



Conclusion

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk.

Activity 1.3 -Security in GSM

Introduction

The main motivation of having a strong security in mobile and wireless communication system are to secure signalling data and conversations from interception and modification as well as to stop and minimize the levels of telephone and wireless fraud

.The security and authentication mechanisms incorporated in GSM make it the most secure mobile communication standard currently available, particularly in comparison to the analog systems described above.

Activity Details

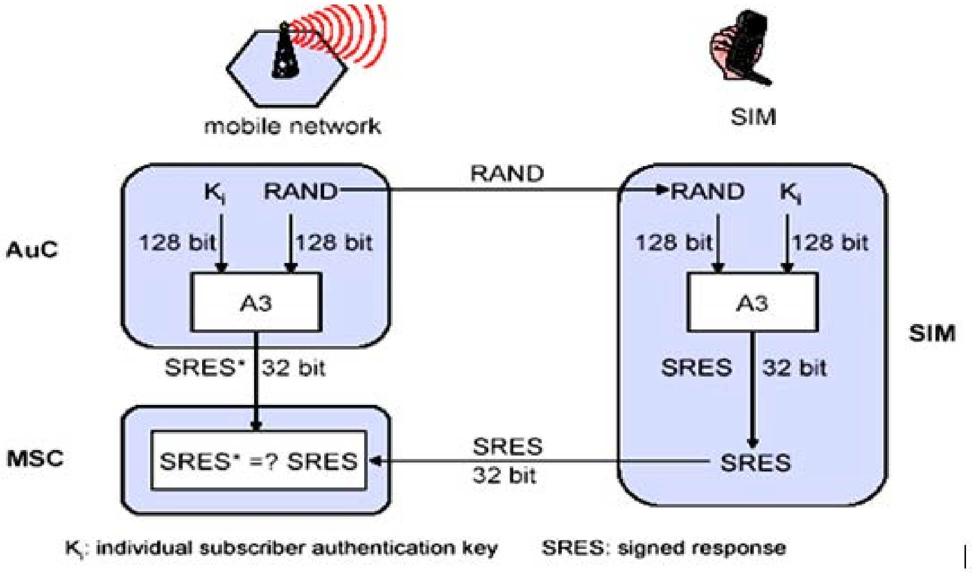
Methods of implementing wireless security

The evolving mobile and wireless communications has to have a lot of security due to the fast growing technology and rise in crime activities.The main objective of communication system is to share data and information with ease and without interruption and reducing threats.This is done using different protocols ,softwares and hardware which proposed to act on security threats .

Wireless networks and security differ in a way that few organization first prefer to have security first then have wireless design so that to evade breakdown in stages of implementation.In the case of GSM ,security is provided by Mobile station Authentication center MSA

Mobile Station Authentication

The subscriber of a network is authenticated by a GSM network through the use of a challenge and response technologies.For a 128-bit Random Number(RAND) which is sent to a mobile station(MS) with 32-bit signed response based 128-bit random number encryption for the authentication algorithm(A3) provided from the Authentication center.A single individual key is used for a specific algorithm.Upon receiving the signed response from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.



Source: http://www.studyinfinity.com/tutorial/mcc/gsm-security.html

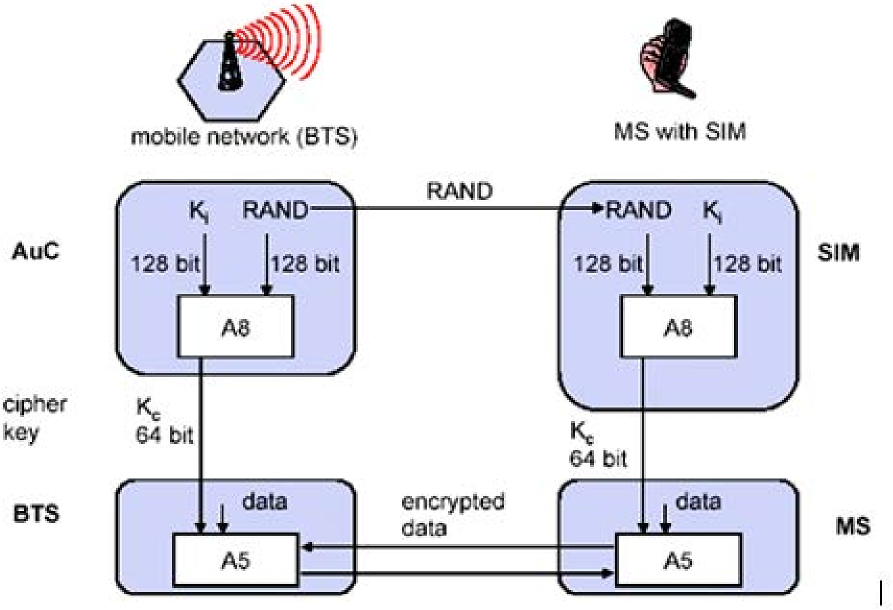
The subscriber authentication key is not transmitted over the same channel since it is available Subscriber Identity module as well as Authentication center ,Home location register and visitor location register database.If the response coincides with the calculated value,then the mobile station is successfully authenticated and and the connection is allowed.If there is a mismatch in the calculated values the connection is terminated and the authentication failure is indicated in a mobile station.

The calculated response within the subscriber identity module provides security as the confidential information such as international mobile subscriber identity and individual authentication key are never released during the authentication process

Signals and confidential data

The ciphering algorithm (A8) is contained in the SIM and it produces a 64-bit ciphering key.The key is calculated by the same random number that used used in the authentication process to the key generation (A8) with a an individual key.

There are also additional level of security that are provided by GSM which is to have the key changed in different sessions and making the system more vulnerable and resistant to attacks.The cipher key can be changed regularly as it may need .FOr the case of calculation of the authentication key ,it is done within the SIM and thus the information such as individual subscriber number key hidden in the sim.



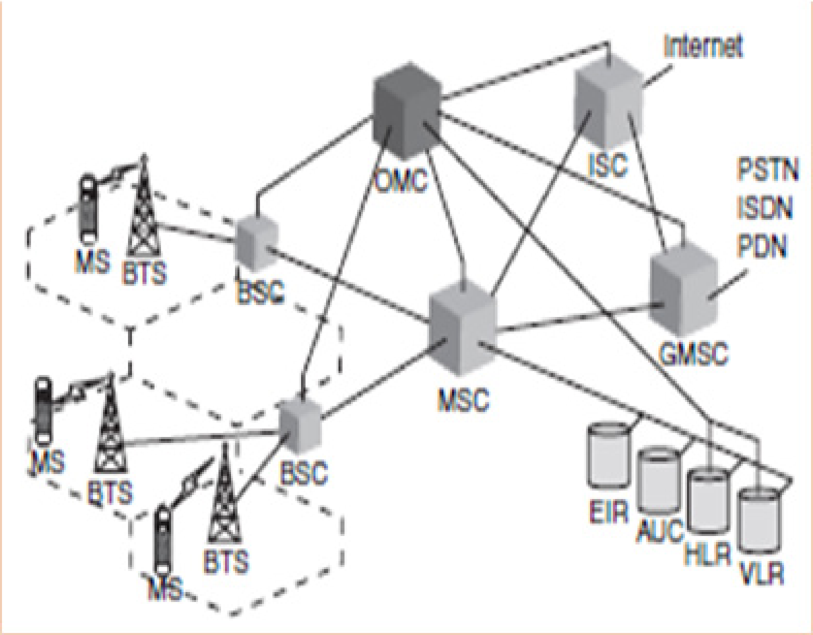
Source:http://www.studyinfinity.com/tutorial/mcc/gsm-security.html

Voice encryption is provided between a mobile station and the network using a ciphering algorithm A5.A ciphering mode request from a GSM network initiates an encrypted network. On the reception of the command the mobile station initiates encryption and decryption of the data using the ciphering Algorithm (A5) and ciphering key.

Confidentiality in subscribing identity

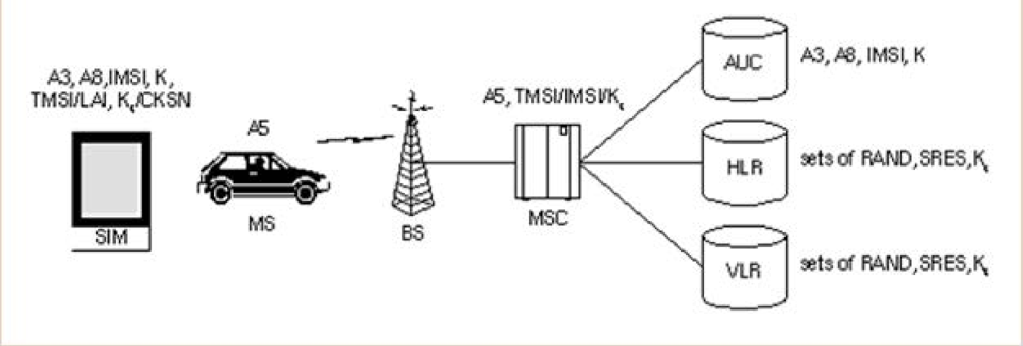
To ensure the confidentiality in gsm a temporary mobile subscriber identity is used .Once the computations of authentication and encryption are done,the temporary mobile subscriber identity is sent to the mobile station after which the mobile station responds.The temporary mobile subscriber identity should be in the valid location which it was issued.For any other external communication that may be necessary A Location area identity may be added for additional temporary mobile subscriber identity.The GSM security mechanisms are implemented by three different elements :

- The Subscriber Identity Module (SIM)
- The GSM handset or Mobile station (MS)
- THe GSM network



The figure above shows the physical architecture of GSM .

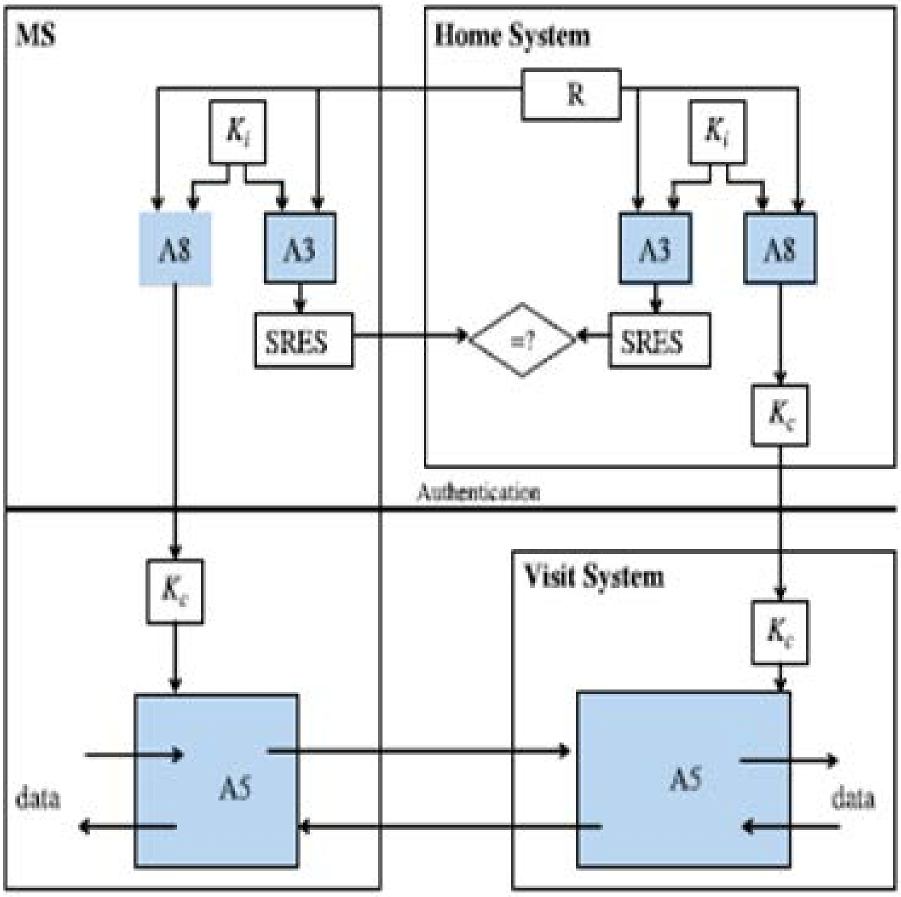
Security features distribution for the three main elements in 2G networks is shown in figure below. The distribution of these security elements give an extra measure of security by providing privacy in mobile networks conversation and prevention of telephone fraud and interruption provide an additional measure of security both in ensuring the privacy of cellular telephone conversations and prevention of cellular telephone fraud.



Source:https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

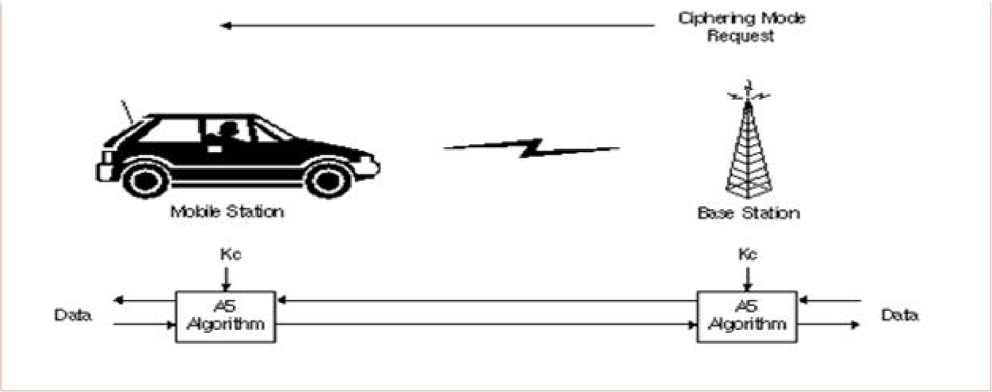
The distribution of algorithm keys in a 2G system is illustrated in the figure below

The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5).



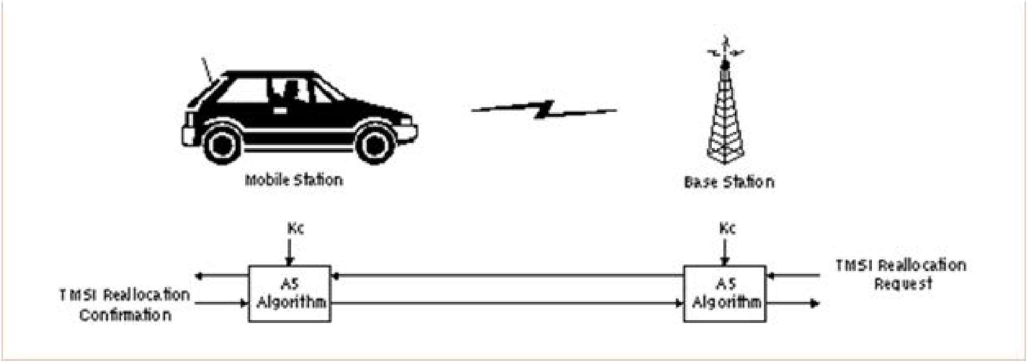
Algorithm and key distribution in GSM

Encryption occurs between the Base Transceiver Station and the Mobile Station without involvement of the home network in the region .For Roaming purposes between different networks the service providers uses encryption algorithm A5 which is provided by the GSM network standard.The computation of ciphering key also happens in the same manner to the authentication key within the SIM.



Source:https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

The Temporary Mobile Subscriber Identity is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the Temporary Mobile Subscriber Identity . If the Temporary Mobile Subscriber Identity is valid in the location area in which it was issued then the access is granted.



Source :https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

Conclusion

The standard mechanism that is used by the GSM makes it the most secure mobile telecomunication system available .The use of encryption ,authentication and identification numbers provides a high level of anonimity as well as safeguarding the system against fraud. Systems with encryption algorithm A8,A5 and A3 are more secure than any other analogue system due to the use of muliple access techniques speech coding and modulation.

Assessment

1. What are the types of cyber crimes committed using cell phones?

   Answer: Subscription Fraud, Cloning, Spoofing, Stalking.

2. What is IMEI?

   Answer: IMEI --- International Mobile Equipment Identity. This is a unique

number,

which identifies a handset. This number will be a single one in the entire world.

This identifies the manufacturer and number of the handset

3. Is it possible to have spoofed SMS? Answer: Spoofing is the process by which the sender’s identity is concealed.

4. Can the location of an anonymous caller be identified?

5. Answer: Yes, It can be identified. The area on which the caller is operating can be identified with the help of service provider.

UNIT SUMMARY

Mobile computing experiences numerous security threats as any other technology.Due to its mobility its is hard to monitor all the security concerns.Different users at different levels can have diverse opinions on how to utilize this privilege.Unlawful and unethical practises such as hacking ,pirating,online fraud and malicious destruction are a few examples of problems experienced in mobile computing.

This Unit has outline and different types of security threats and attacks and some ways in which they are secured.

Unit Assessment

Check your understanding!

1. a. Describe the four major threats to the security of wireless networks.4 Marks

   b.Which of these threats is the most dangerous for a business?

   which is the most dangerous for an individual? Support your answers. (6 marks)

2. Describe Localization and calling in GSM(5 marks) Describe Handoff in cellular networks.(5 marks)

3. Differentiate between Symmetric and asymmetric cryptosystems(4 marks)

4. Outline the two methods of implementing wireless security(6 marks)

Solution Manual

1. The four threats are rogue access points, wardriving, eavesdropping and RF jamming.

2. The most dangerous threats for a business are war driving and RF jamming. For individuals, rogue access points are the most serious threat, particularly at public hotspots. Eavesdropping is threatening for both business and individual networks.

3. Worldwide localization of users and roaming are the main service provided by the GSM network system. The system always knows where a user currently is, and the same phone number is valid worldwide. For providing this service GSM updates the user location periodically. The HLR always contains information about the current location. VLR responsible for the MS informs the HLR about location changes. As soon as an MS moves into the new location area (range of new VLR), the HLR sends all user information needed to the new VLR.

4. When a user talks on the mobile phone to another user it may happen that the mobile station moves from one cell to another. During this conversation signal may become weak. To solve this problem, the Mobile Switching Center (MSC) checks the level of the signal every few seconds. If the strength of the signal is week then the MSC searches a new cell that can provide better communication.

Handoff is the process by which a mobile telephone call is transferred from one base

station to another base station

5. There are two types of cryptosystems which depend on the key uses.Asymmetric cryptosystem uses different keys for encryption and symmetric cryptosystem uses single key for both encryption and decryption.

A key gives us flexibility in using an encryption scheme. We can create different encryptions of one plaintext message just by changing the key. Moreover, using a key provides additional security. If the encryption algorithm should fall into the interceptor's hands, future messages can still be kept secret because the interceptor will not know the key value.

6. The evolving mobile and wireless communications has to have a lot of security due to the fast growing technology and rise in crime activities.The main objective of communication system is to share data and information with ease and without interruption and reducing threats.This is done using different protocols ,softwares and hardware which proposed to act on security threats .

Wireless networks and security differ in a way that few organization first prefer to have security first then have wireless design so that to evade breakdown in stages of implementation.In the case of GSM ,security is provided by Mobile station Authentication center MSA

Instructions

Answer all the questions

Grading Scheme

Question 1 (10 marks)

Question 2 (5 marks)

Question 3 (5 marks)

Question 4 (4 marks)

Question 5(6 marks)

Unit Readings and Other Resources

1. https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

2. Kahate, A. (2013). Cryptography and network security. Tata McGraw-Hill Education.

3. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., & Srivastava, M. B. (2002). On communication security in wireless ad-hoc sensor networks. InEnabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on(pp. 139-144). IEEE.

4. Rappaport, T. S. (1996). Wireless communications: principles and practice(Vol. 2). New Jersey: Prentice Hall PTR.

5. http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm_architecture.php

Course References

1. Kahate, A. (2013). Cryptography and network security. Tata McGraw-Hill Education.

2. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., & Srivastava, M. B. (2002). On communication security in wireless ad-hoc sensor networks. InEnabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on(pp. 139-144). IEEE.

3. Rappaport, T. S. (1996). Wireless communications: principles and practice(Vol. 2).

4. New Jersey: Prentice Hall PTR.

5. http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm_architecture.php

6. http://slideplayer.com/slide/6009611/

7. Eberspächer, J., Vögel, H. J., Bettstetter, C., & Hartmann, C. (2008). GSM-architecture, protocols and services. John Wiley & Sons.

8. Yacoub, M. D. (2001). Wireless technology: protocols, standards, and techniques. CRC press.

9. https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

The African Virtual University Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

The African Virtual University Regional Office in Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org