الجمهوريــة الجزائريــة الديمقراطيــة الشعبيــة

People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

University of Relizane **جامعة غليزان**

Faculty of Science and Technology

Computer Science Department

COURSE MATERIAL

Emerging Networks

For students of the 2nd year Master speciality:

Networks and Distributed Systems

Prepared by:

Dr. Oussama DERNI

oussama.derni@univ-relizane.dz

2024/2025

Preface

This course is designed to familiarize students with emerging technologies and their applications in modern information and communication techniques, including RFID, wireless sensor networks, and GSM networks. Targeted at second-year Master's students in Computer Science, specializing in "Networks and Distributed Systems," the course begins by covering fundamental access protocols and the concept of QoS in WLANs. It then explores the evolution of next-generation wireless networks, such as IEEE 802.11, 802.15, and 802.16. Additionally, it addresses routing and QoS in ad hoc networks, followed by a focus on wireless sensor networks, their key applications, routing, and security. The course concludes with a discussion on vehicular networks and network security.

On completion of this course, students will be able to:

- **Explain** the different wireless networks and their evolution
- **Acquire** a basic understanding of access protocols in WLANs
- **Discuss** the main axes of ad hoc networks
- **Understand** wireless sensor networks
- **Emphasize** the essential notions of vehicular networks
- **Summarize** the main techniques for securing networks

Learners are required to:

- Have a basic understanding of computer networks
- An understanding of fiber optic technology
- Knowledge of radio waves

Chapter 01 • State of the art and evolution of wireless networks

Chapter 02 • WLAN access protocols and QoS

Chapter 03 • Ad hoc networks : MANET

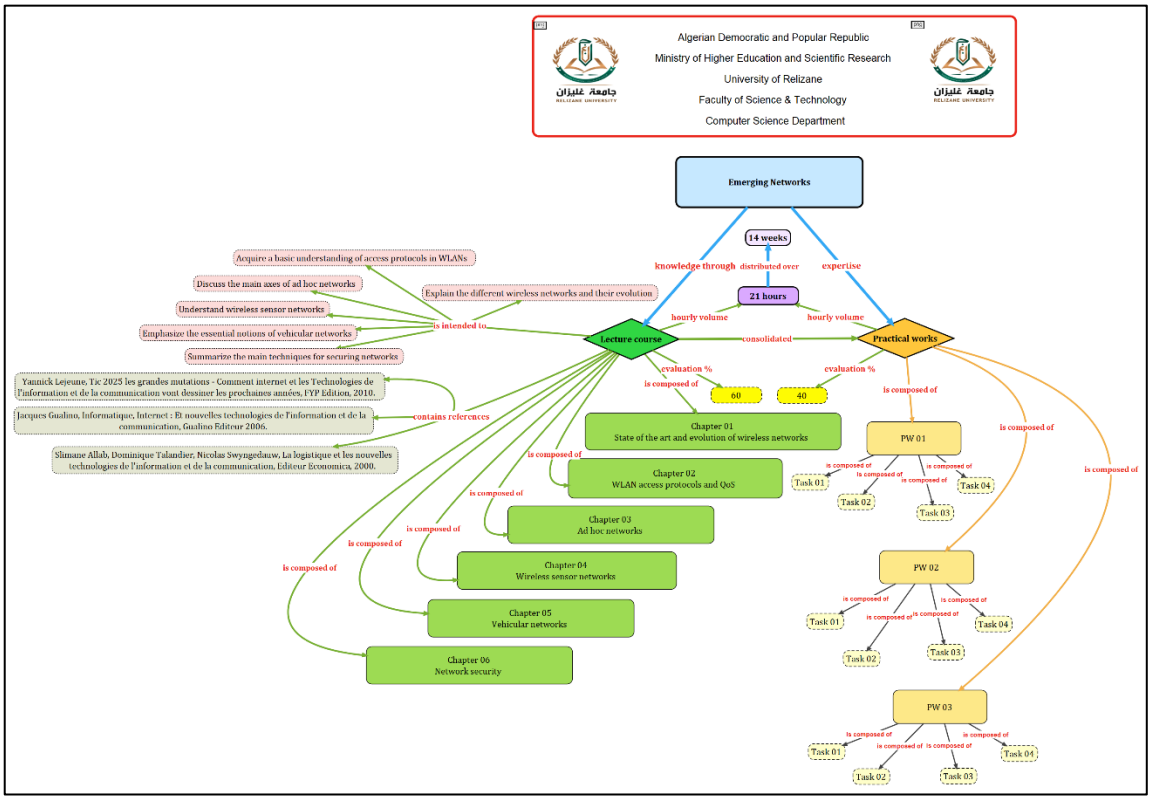
Chapter 04 • Wireless sensor networks

Chapter 05 • Vehicular networks

Chapter 06 • Network security

Conceptual map

It provides an organized structure for understanding how the topics of this course are interconnected. This map is used to help both instructors and students better grasp the overall flow and hierarchy of the subject matter.



Contact sheet

Establishment	University of Relizane
Faculty	Science and Technology
Department	Computer Science
Target audience	2nd year Master, Networks and Distributed Systems specialization
Course title	Emerging Networks
Teaching unit	Fundamental
Credits	04
Coefficients	02
Duration	14 weeks
Evaluation method	Exam (60%), Continuous (40%)
Total hourly volume	(21h Course, 21h Practical work)
Course schedule	Monday, 10:00 to 11:30 a.m.
Teacher in charge	Dr. Oussama DERNI
Contact	oussama.derni@univ-relizane.dz
Availability	Monday and Wednesday (teachers' room)

TABLE OF CONTENTS

PREFACE ..... **II**

CONCEPTUAL MAP ..... **IV**

CONTACT SHEET ..... **V**

TABLE OF CONTENTS ..... **VI**

LIST OF FIGURES ..... **X**

LIST OF TABLES ..... **XI**

CHAPTER 01 : STATE OF THE ART AND EVOLUTION OF WIRELESS NETWORKS **12**

1.1. INTRODUCTION 12

1.2. WIRELESS NETWORK TYPES 12

1.2.1. Wireless personal area network (WPAN) *13*

1.2.2. Wireless local area network (WLAN) *13*

1.2.3. Wireless metropolitan area network (WMAN) *13*

1.2.4. Wireless Wide Area Network (WWAN) *13*

1.3. EVOLUTION OF WIRELESS NETWORKS 14

1.3.1. WPAN (Bluetooth evolution) *14*

1.3.2. WLAN (Wi-Fi evolution) *16*

1.3.3. WMAN (WiMAX evolution) *18*

1.3.4. WWAN (cellular network evolution) *20*

CHAPTER 02 : ACCESS PROTOCOLS AND QOS IN WLANS **25**

2.1. INTRODUCTION 25

2.2. WLAN APPLICATIONS 25

2.2.1. Healthcare sector *25*

2.2.2. Day-to-day business *25*

2.2.3. In-building network managers *25*

2.2.4. Network operators in dynamic environments *25*

2.3. WLAN ACCESS PROTOCOLS 26

2.3.1. Data link control *26*

2.3.2. Multiple access control *26*

2.4. QOS IN WLAN NETWORKS 30

2.4.1. QoS privileges *30*

2.4.2. How does QoS work? *31*
2.4.3. QoS metrics *32*
2.4.4. Techniques involved in QoS *32*
2.4.5. The 802.11e standard *33*
2.4.6. QoS at Layer 3 ..... *34*

CHAPTER 03 : AD HOC NETWORKS: MANET 36

3.1. INTRODUCTION 36
3.2. DEFINITION: MOBILE AD HOC NETWORKS 36
3.3. CHARACTERISTICS 37
3.4. ROUTING IN MANETS 38
3.4.1. Classification of routing protocols *38*
3.4.2. The AODV protocol *40*
3.5. QOS IN AD HOC NETWORKS 44
3.5.1. CEDAR *44*
3.5.2. QoS AODV *45*
3.5.3. Bandwidth routing *45*
3.5.4. On-Demand QoS Routing *45*

CHAPTER 04 : WIRELESS SENSOR NETWORKS 46

4.1. INTRODUCTION 46
4.2. DEFINITION: WIRELESS SENSOR NETWORKS 46
4.3. MAIN APPLICATIONS 47
4.4. WSN COMPONENTS 47
4.5. SENSOR NODE ARCHITECTURE 48
4.6. DESIGN CHALLENGES IN WSNS 50
4.6.1. Energy efficiency *50*
4.6.2. Complexity *50*
4.6.3. Scalability *50*
4.6.4. Delay *50*
4.6.5. Robustness *50*
4.6.6. Data transmission and transmission models *51*
4.6.7. Sensor location *51*
4.7. MAC LAYER STUDIES FOR SENSOR NETWORKS 51
4.7.1. IEEE 802.11 ..... *52*
4.7.2. S-MAC *52*
4.7.3. T-MAC *53*
4.8. ROUTING IN SENSOR NETWORKS 53

4.8.1. Node-centric *54*
4.8.2. Data-centric *54*
4.8.3. Destination-initiated protocols *55*
4.8.4. Source-initiated *55*
4.9. BROADCAST PROTOCOLS FOR SENSOR NETWORKS 55
4.9.1. Low energy adaptive clustering hierarchy (LEACH) *55*
4.9.2. LEACH communication architecture *56*
4.9.3. How LEACH works *56*
4.9.4. TEEN (Threshold sensitive Energy Efficient sensor Network protocol) *57*
4.10. ENERGY MANAGEMENT FOR SENSOR NETWORKS 58
4.10.1. Forms of energy dissipation *58*
4.10.2. Factors involved in energy consumption *58*
4.10.3. Energy conservation techniques *59*
4.11. OVERVIEW OF OPERATING SYSTEMS FOR SENSOR NETWORKS (TINYOS EXAMPLE) 61
4.11.1. TinyOS features *61*
4.11.2. Overview of TinyOS *62*
4.11.3. TinyOS memory model *62*
4.12. SYNCHRONIZATION IN SENSOR NETWORKS 63
4.12.1. Reference Broadcast Synchronization *64*
4.13. SECURITY IN SENSOR NETWORKS 64
4.13.1. Attacks and solutions in WSNs *64*

CHAPTER 05 : VEHICULAR NETWORKS 67

5.1. INTRODUCTION 67
5.2. MAIN APPLICATIONS 67
5.3. STUDY OF THE MAC AND PHYSICAL LAYER 68
5.3.1. IEEE standards for mac protocols (VANET) *69*
5.4. ROUTING IN VEHICULAR NETWORKS 73
5.4.1. Topology-based routing protocols *74*
5.4.2. Position-based routing protocols *75*
5.4.3. OLSR *75*
5.4.4. GPSR *76*
5.5. MOBILITY MODEL AND SIMULATION 77
5.5.1. Macroscopic mobility model *77*
5.5.2. Microscopic mobility model *78*
5.6. VANET SECURITY 80
5.6.1. Attack classification and proposed solutions *80*

CHAPTER 06 : NETWORK SECURITY 82

6.1. INTRODUCTION 82

6.2. SINGLE SIGN-ON (SSO) 82

6.2.1. How it works? 82

6.2.2. The SSO token 83

6.3. DNS SECURING DNS 83

6.3.1. Major attacks 83

6.4. SECURITY FOR WI-FI WIRELESS NETWORKS 85

6.4.1. Strong passwords 85

6.4.2. Robust Encryption 85

6.4.3. Network Isolation 85

6.4.4. Secure Connections 86

6.4.5. Regular Monitoring 86

6.5. SECURING DIGITAL MEDIA ON THE INTERNET (DRM 'DIGITAL RIGHT MANAGEMENT') 86

6.5.1. Techniques used 86

6.6. E-MAIL SECURITY, ANTI-SPAM MECHANISMS (STATISTICAL FILTERING MECHANISMS) 87

6.6.1. Anti-spam mechanisms 87

6.6.2. Heuristics 88

6.6.3. Bayesian filtering 88

6.7. SECURITY IN WEB SERVICES 88

6.7.1. XML-Signature 88

BIBLIOGRAPHY 90

LIST OF FIGURES

Figure 1.1. Cellular network 21
Figure 1.2. GSM architecture 22
Figure 2.1. IEEE 802.11 Access Layer 26
Figure 2.2. Multiple access protocols 27
Figure 3.1. Ad hoc network 37
Figure 3.2. Classification of routing protocols in ad hoc networks 38
Figure 3.3. Broadcasting RREQ packet: reverse path creation 42
Figure 3.4. RREP response to the source node 43
Figure 3.5. RERR generation due to node B failure 44
Figure 4.1. Sensor architecture 48
Figure 4.2. Basic schematic for S-MAC 53
Figure 4.3. Basic schematic for T-MAC 53
Figure 4.4. Classification of WSNs routing protocols 54
Figure 4.5. LEACH protocol communication architecture 56
Figure 4.6. Energy conservation techniques 60
Figure 4.7. A set of software components 62
Figure 5.1. Example of a vehicular network 67
Figure 5.2. DSRC spectrum allocation in the USA. 69
Figure 5.3. The WAVE protocol stack. 70
Figure 5.4. Reference architecture for MAC channel coordination 71
Figure 5.5. Time division into CCH intervals and SCH intervals, IEEE 1609.4 standard 72
Figure 5.6. V2I and V2V structure 74
Figure 5.7. VANET routing protocols 74
Figure 5.8. Flooding a packet in a multi-hop wireless network from the central node using MPR 76
Figure 5.9. VanetMobiSim 80
Figure 5.10. Classification and examples of VANET attacks 81
Figure 6.1. SSO operations 83
Figure 6.2. A hybrid attack 85

LIST OF TABLES

Table 1.1. Types of wireless networks 12
Table 2.1. LWAPP packets and QoS marking 35
Table 3.1. Format of an RREQ 40
Table 3.2. Format of an RREP 40
Table 3.3. Format of HELLO message 40
Table 3.4. Format of an RERR 41
Table 5.1. IEEE 802.11p parameter settings for different application categories 73
Table 5.2. Major attacks, cryptographic solutions and proposals. 81

Chapter 01 : State of the art and evolution of wireless networks

1.1. Introduction

Wireless networks are computer networks that are not connected by any type of cable. Using a wireless network enables companies to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems is radio waves, an implementation that takes place at the physical level of the network structure. In this chapter, we'll look at the different types of wireless networks and their chronological evolution.

1.2. Wireless network types

One way of categorizing the different types of wireless network designs is by their scope or scale. For historical reasons, the networking industry refers to almost all design types as some kind of area network.

- WPAN - Wireless Personal Area Network
- WLAN - Wireless Local Area Network
- WMAN - Wireless Metropolitan Area Network
- WWAN - Wireless Wide Area Network

Table 1.1. Types of wireless networks

Type	Range	Applications	Standards
Wireless personal area network (WPAN)	Within reach of one person	Replacing cables for peripherals	Bluetooth, ZigBee, NFC
Wireless local area network (WLAN)	In a building or on a campus	Wireless extension of wired network	IEEE 802.11 (Wi-Fi)
Wireless Metropolitan Area Network (WMAN)	Within a city	Inter-network wireless connectivity	IEEE 802.16 (Wi-MAX)
Wireless wide area network (WWAN)	On a global scale	Wireless network access	Cellular (UMTS, LTE, etc.)

1.2.1. Wireless personal area network (WPAN)

A Personal Area Network (PAN) connects electronic devices in a user's immediate area. The size of a PAN varies from a few centimeters to a few meters. One of the most common examples of a PAN in the real world is the connection between a Bluetooth headset and a smartphone. A wireless personal area network (WPAN) is a group of devices connected without the use of wires or cables. Today, most PANs in everyday use are wireless. WPANs use short-range wireless connectivity protocols. Wireless connection methods include Bluetooth (the most common), WIFI, IrDA and Zigbee.

1.2.2. Wireless local area network (WLAN)

A wireless local area network (WLAN) is a group of co-located computers or other devices that form a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN. WLANs use high-frequency radio waves and often include an Internet access point. A WLAN enables users to move around the coverage area, often a home or small office, while maintaining a network connection.

1.2.3. Wireless metropolitan area network (WMAN)

The Wireless Metropolitan Area Network (WMAN) is a type of Metropolitan Area Network (MAN), the only thing being that the connectivity is wireless. It extends over several locations in a geographical area and serves a range of over 100 meters. It's a type of wireless network with a coverage area about the size of a city. Typically, it extends or covers an area larger than the wireless local area network (WLAN) but smaller than the wireless wide area network (WWAN). WMAN connections can be point-to-point or point-to-multipoint networks. It's a newer networking technology that complements certain wired technologies such as Gigabit Ethernet and SONET over IP. WMAN technologies include Wi-MAX, LMDS and MMDS.

1.2.4. Wireless Wide Area Network (WWAN)

A Wireless Wide Area Network (WWAN) is a specific type of network that sends wireless signals beyond a building or property. Wireless WANs and wireless LANs also differ in the types of signal processing technologies they use. A WWAN can use various types of cellular network systems to send signals over a longer distance. Large telecoms providers like Algeria telecom usually support a wireless WAN in one way or another, and these large network types often require certain types of encryptions or security that a local

network may not need. WWANs use cellular telecommunications network technologies such as 2G, 3G, 4G LTE and 5G to transfer data.

WWANs are network traffic encapsulated in a mobile communications technology such as Worldwide Interoperability for Microwave Access (WIMAX), Universal Mobile Telecom System (UMTS), code division multiple access (CDMA) 2000, Global System for Mobile (GSM) or 3G networks to name just a few. The cellular mobile telecommunications network enables users with WWAN cards or integrated cellular radios (GSM/CDMA) to surf the Web, send and receive e-mails and, in general, perform any networking function as if they were physically connected to a WAN.

1.3. Evolution of wireless networks

Wireless network technologies have evolved over the last few decades, so for each type of wireless network we'll take the most widely used technology and examine their evolution chronologically.

1.3.1. WPAN (Bluetooth evolution)

Today, most everyday PANs are wireless. WPANs use short-range wireless connectivity protocols such as Bluetooth. Bluetooth technology enables devices to communicate with each other without cables or wires. Bluetooth is based on a short-range radio frequency, and any device incorporating the technology can communicate as long as it is within the required distance. Bluetooth operates on a band frequency of 2.4 gigahertz (GHz), and Bluetooth connectivity is based on the packet-based protocol, which involves dividing data into packets and transmitting each packet on one of 79 designated Bluetooth channels.

1.3.1.1. Bluetooth 1.0

- This is the first version created in 1999

1.3.1.2. Bluetooth 1.1

- Released in 2002
- Bug fixes
- Use of unencrypted channels now possible
- Addition of a signal to measure reception power

1.3.1.3. Bluetooth 1.2

- Released in 2003
- Higher practical data rate of 721 kbit/s and improved resistance to interference

1.3.1.4. Bluetooth 2.0

- Released in 2004
- Higher practical throughput
- Backward compatibility
- Reduced peripheral consumption and optimized transfers

1.3.1.5. Bluetooth 2.0+EDR

- Released in 2004
- Theoretical maximum data rate increased to 3 Mbit/s (2.1 Mbit/s useful) with EDR (Enhanced Data Rate) mode

1.3.1.6. Bluetooth 2.1+EDR

- Released in 2007
- Easier, faster coupling.
- Enhanced security
- Addition of an NFC (Near Field Communication) connection mode to facilitate pairing at very short range.

1.3.1.7. Bluetooth 3

- Released in 2009
- Theoretical higher data rate increased to 2.1Mbit/s in "HS" high-speed mode

1.3.1.8. Bluetooth 4 + LE (creation)

- Released in 2010
- **Bluetooth classic:** inferior changes
- **Bluetooth LE**:
    - Reduced peripheral power consumption (Low Energy)

1.3.1.9. Bluetooth 4.2

- Released in 2014
- **Bluetooth classic:** inferior changes
- **Bluetooth LE:**

- Reduced consumption of secure IP protocols for connected objects.
- Increase in useful packet size (PDU) from 31 to 256 bytes, significantly reducing download times.

1.3.1.10. Bluetooth 5

- Released in 2016
- **Classic Bluetooth:** Reduces interference with other devices
- **Bluetooth LE**
  - Higher theoretical data rate (2 Mbit/s PHY), practical: 1.4 Mbit/s, range from 40 m to 350 m and up to 500 meters with certain modules.

1.3.1.11. Bluetooth 5.1

- Released in 2019
- **Classic Bluetooth:** angle of arrival and departure, used to geolocate devices
- **Bluetooth LE:**
  - Ability for a device to determine the direction of the Bluetooth signal (localization)

1.3.1.12. Bluetooth 5.3

- Released in 2021
- More energy-efficient

1.3.2. WLAN (Wi-Fi evolution)

Wi-Fi is a wireless network technology that enables devices such as computers (laptops and desktops), mobile devices (smartphones and cell phones) and other equipment (printers and video cameras) to interface with the Internet. It enables these devices - and many others - to exchange information with each other, creating a network. Internet connectivity is achieved via a wireless router. When you access Wi-Fi, you connect to a wireless router that enables your Wi-Fi-compatible devices to interface with the Internet.

1.3.2.1. IEEE 802.11

IEEE 802.11 is a standard developed by the Institute of Electrical and Electronic Engineers (IEEE). It is the original wireless specification. Extensions to the 802.11 standard have been given the same number with a letter suffix. 802.11 Provides up to 2 Mbps transmission in the 2.4 GHz band.

1.3.2.2. IEEE 802.11b

It worked in the 2.4 GHz frequency, like the original 802.11 standard. With a maximum range of 40 meters and a speed of 11 Mbps. One of the main drawbacks of this standard was that, as its operating frequency is 2.4 GHz, just like other household appliances, the risk of them causing interference was greater. Currently, routers that support this standard are not even being manufactured.

1.3.2.3. IEEE 802.11a

Released at almost the same time as 802.11b, it came with a more advanced and complex technology. It relied on orthogonal frequency division multiplexing to generate wireless signals. It operated in the 5 GHz frequency range and offered multiple advantages, including the elimination of interference from other devices. It also offered incremental bandwidth, providing connectivity speeds of around 54 Mbps.

1.3.2.4. IEEE 802.11g (Wi-Fi 3)

Four years later, another standard was defined by the committee. This was a time when Wi-Fi standards were improving and devices were advancing to support higher ranges, power, bandwidth and coverage. In 2003, 802.11g was introduced and functioned exactly like 802.11a. This meant that it operated on orthogonal frequency division multiplexing technology, but the only drawback it faced was that it fell back into the 2.4 GHz spectrum, again raising concerns about interference. However, 802.11g came with backwards compatibility features, in which the 802.11b router could connect to an 802.11g access point but at 802.11b speeds.

1.3.2.5. IEEE 802.11n (Wi-Fi 4)

In 2009, 802.11n arrived to simply give the market what it was looking for. Using multiple-input, multiple-output technology, this standard offered a fantastic speed of 300 Mbps. Because it worked on this technology, speeds of 450 Mbps could even be achieved with the inclusion of more antennas. It operated in the 2.4 GHz and 5 GHz spectrums, enabling users to benefit from greater data transmission power without the need for higher bandwidth.

1.3.2.6. IEEE 802.11ac (Wi-Fi 5)

2014 was the year of a remarkable achievement in terms of Wi-Fi standards. 802.11ac was introduced, and this new technology could offer speeds ranging from 433Mbps to several gigabytes per second. Operating only in the 5 GHz spectrum, this technology supports up to 8 spatial streams and increases channel width up to 80 MHz with 802.11ac, a new technology called beamforming was introduced. With this, signals from a device's antennas could be directed to a specific device. In addition, this standard also added a layer to the concepts of multiple inputs and multiple outputs. Whereas multiple streams could be directed to a single client in 802.11n, 802.11ac allowed multiple streams to be directed to multiple clients at once.

1.3.2.7. IEEE 802.11ad

This standard was introduced in 2018. Using beam-forming technology, this technology operates in the 60 GHz frequency band (covers the frequency from 57 to 71 GHz) and offers speeds of up to 7Gbps. This brings us to another crucial technology, based essentially on wireless technology. Six channels are available, each with a nominal bandwidth of 2.16 GHz. Channel 2 (59.40-61.56 GHz) is available in all regions and is considered the default channel.

1.3.2.8. IEEE 802.11ax (Wi-Fi 6)

The next-generation 802.11ax Wi-Fi standard, also known as Wi-Fi 6, is the latest step in a journey of continuous innovation. The standard builds on the strengths of 802.11ac, adding the efficiency, flexibility and scalability that enable new and existing networks to increase speed and capacity with next-generation applications. IEEE proposed this standard to couple the freedom and high speed of Gigabit Ethernet wireless with the reliability and predictability found in licensed radio. The IEEE 802.11ax standard was finalized in September 2020.

1.3.2.9. IEEE 802.11be (Wi-Fi 7)

Expected for full release in 2024, Wi-Fi 7 will bring faster speeds, reduced latency, and improved network capacity. It will use 320 MHz channels and support multi-link operation (MLO) to combine multiple frequencies for better performance in dense environments.

1.3.3. WMAN (WiMAX evolution)

WiMAX is one of today's most popular broadband wireless technologies. WiMAX systems are expected to deliver broadband access services to residential and business customers in a cost-effective way. WiMAX is a standardized wireless version of Ethernet designed primarily to replace wired technologies (such as cable modems, DSL and T1/E1 links) to provide broadband access to customer premises. More strictly, WiMAX is an industry trade organization formed by leading communications, components and equipment companies to promote and certify the compatibility and interoperability of broadband wireless access equipment compliant with IEEE 802.16 and ETSI HIPERMAN standards. WiMAX is said to work like Wi-Fi, but at higher speeds over greater distances and for more users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to access, and the ability to overcome the physical limitations of traditional wired infrastructure. WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 what the Wi-Fi Alliance is to 802.11.

1.3.3.1. IEEE 802.16

This is a family of IEEE standards for wireless broadband access. Approved in 2002, and also known as "WiMAX", 802.16 provides up to 300 Mbps point-to-multipoint shared transmission in frequency bands from 10 to 66 GHz up to 30 kilometers. At frequencies below 11 GHz, signals can penetrate walls and other dense objects.

1.3.3.2. IEEE 802.16a

IEEE 802.16a is a computer communications standard ratified on January 29, 2003, specifying a type of wireless data transmission at data rates of up to 70 Mbps over a frequency band between 2 and 11 GHz. It is also an amendment to the 802.16 standard for wireless metropolitan area networks (WMAN). Channel bandwidth is 1.25 to 28MHz. It has a maximum range of 50km.

1.3.3.3. IEEE 802.16-2009

The IEEE 802.16-2009 standard defines a generic reference model in which the main functional blocks (i.e., the physical layer, the security sublayer, the MAC common part sublayer and the service-specific convergence sublayer) and their interfaces, the IEEE 802.16 entity premises, and a general network control and management system are specified.

1.3.3.4. IEEE 802.16m

It achieves data rates of 100 Mbit/s mobile and 1 Gbit/s fixed. Also known as Mobile WiMAX Release 2 or Wireless-MAN-Advanced. Aimed at meeting ITU-R IMT-Advanced requirements for 4G systems. 802.16m modified the reference model (802.16-2009) by classifying MAC common part sublayer functions into two functional groups, resulting in a more structured approach to characterizing data link layer functions and their interworking.

1.3.4. WWAN (cellular network evolution)

WWAN (Wireless Wide Area Network) is a WAN (Wide Area Network), the only difference being that the connectivity is wireless. It offers regional, national and global wireless coverage. Where the WAN can be wired or wireless, wireless WAN connections are entirely wireless. In our daily lives, we use the wireless WAN in various sizes and, depending on the delivery of phone calls, web pages and video, data sharing occurs.

WWAN uses cellular telecommunications network technologies such as 2G, 3G, 4G LTE and 5G to transfer data.

The cellular network is a communications network specifically designed for mobile equipment. It enables communication between these mobile units and with all subscribers. The radio wave in a cellular network is the link between the mobile and the transmitter infrastructure. The technology was developed for mobile radiotelephony to replace high-power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

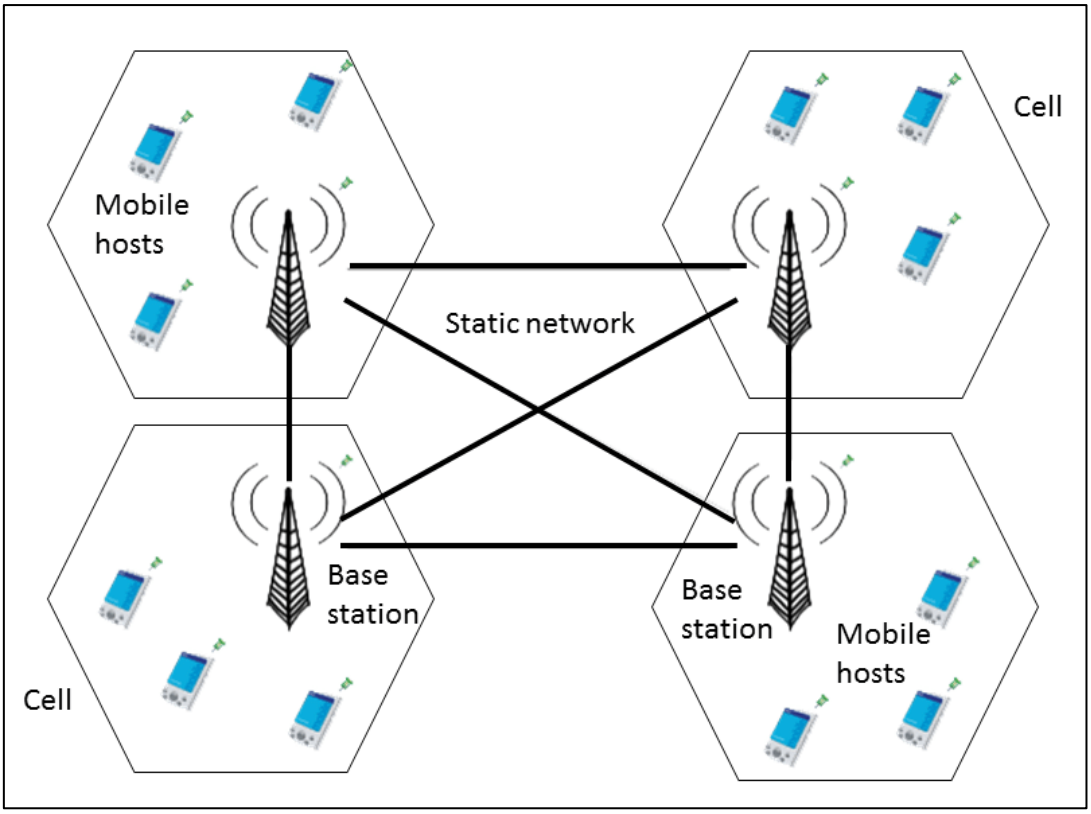


Figure 1.1. Cellular network

1.3.4.1. GSM (Global System for Mobile Communication)

It is a digital cellular technology used to transmit mobile voice and data services. The GSM concept emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s. GSM is also the name of a standardization group set up in 1982 to create a common European standard for mobile telephony. GSM is the most widely accepted telecommunications standard, and is implemented worldwide. GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time slots. It operates on the 900 MHz and 1800 MHz mobile communications bands in most parts of the world. In Algeria, GSM operates in the 880-890/925-935 MHz bands. It has a market share of over 70% of digital cellular subscribers worldwide. GSM uses narrow-band Time Division Multiple Access (TDMA) technology to transmit signals. GSM was developed using digital technology and provides advanced basic voice and data services, including roaming. Roaming is the ability to use your GSM phone number in another GSM network.

1.3.4.1.1. Architecture

The GSM system is made up of four components

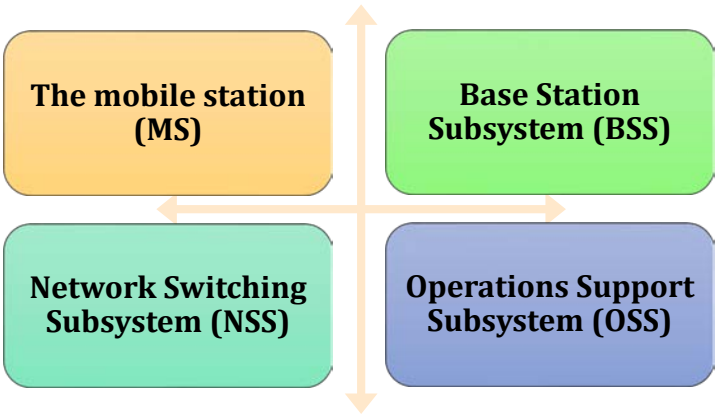


Figure 1.2. GSM architecture

The mobile station (MS): It consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card.

Base Station Subsystem (BSS): Consists of two parts:

- The base transceiver station (BTS): corresponds to the transceiver antennas used in each network cell.
- Base Station Controller (BSC): manages radio resources for one or more BTSs. It manages radio channel configuration, frequency hopping and handovers.

Network Switching Subsystem (NSS): The main part is the Mobile Switching Center (MSC), which switches calls between the mobile and other users of the fixed or mobile network, as well as managing mobile services such as authentication.

Operations Support Subsystem (OSS): The functional entity from which the network operator monitors and controls the system. The aim of OSS is to offer the customer cost-effective support for the centralized, regional and local operation and maintenance activities required for a GSM network.

1.3.4.2. UMTS (Universal Mobile Telecommunications System)

Based on GSM standards, this is a third-generation mobile cellular system maintained by 3GPP (3rd Generation Partnership Project). It specifies a complete network system, and the technology it describes is commonly referred to as freedom of mobile multimedia access (FOMA).

1.3.4.3. GPRS (General Packet Radio Service)

GPRS introduces packet data transmission to the mobile subscriber. It is designed to operate within the existing GSM infrastructure with additional packet switching nodes.

This packet-based technique uses multi-slot technology and support for all coding schemes to increase data rates up to 160 kbit/s.

The GPRS system uses physical radio channels as defined for GSM. A physical channel used by GPRS is called a packet data channel (PDCH). PDCHs can either be allocated for GPRS (dedicated PDCH), or used by GPRS only if no circuit-switched connection requires them (on-demand).

1.3.4.4. EDGE (Enhanced Data rates for Global Evolution)

Introduces a new modulation technique and protocol improvements for radio packet transmission. It offers considerable throughput and capacity gains, enabling 3G services in existing GSM/GPRS networks. No changes are required to the existing core network infrastructure to support EDGE. This underlines the fact that EDGE is simply an add-on for BSS.

1.3.4.5. 1G

1G refers to the first generation of wireless telephony technology. 1G is an analog technology, and phones using it had poor battery life and voice quality, little security, and were prone to dropped calls. The maximum speed of 1G technology is 2.4 Kbps.

It was introduced in 1979 and in the early to mid-1980s, when it was replaced by 2G digital telecommunications. The main difference between these two generations of cell phones is that in 1G systems, audio was encoded as analog radio signals, while 2G networks were entirely digital.

1.3.4.6. 2G

In 2G, roaming and SMS messaging were introduced and later enhanced with GPRS for data communication. SMS messaging and GPRS became widely used for basic telemetry. Roaming has made mobile technology suitable for multi-country deployments. 2G/Edge offers a theoretical maximum data rate of 384 Kbps.

1.3.4.7. 3G

Networks based on 3G connections were introduced in 2001, marking the start of widespread use of the Internet on cell phones. 3G became a truly global standard, combining the best of competing technologies into a single standard. Developments in 3G were mainly focused on high-speed data applications. 3G data technology uses a network of telephone towers to transmit signals, ensuring a stable and relatively fast connection

over long distances. The tower closest to the user's cell phone transmits the data to it. Although it may not sound complex, 3G technology was revolutionary when it was first introduced.

1.3.4.8. 4G

The introduction of 4G has truly ushered in the era of the smartphone and the portable mobile device. 4G is the first generation to use Long-Term Evolution (LTE) technology to deliver theoretical download speeds of between 10 Mbps and 1 Gbps, offering end-users better latency (less buffering), improved voice quality, instant messaging and social media services, quality streaming and faster download speeds. 4G is also the first IP-based mobile network, treating voice as a simple service, and the technology is being developed to meet the quality of service (QoS) and throughput requirements demanded by applications including wireless broadband access, multimedia messaging service (MMS), video chat, mobile TV, HDTV content, digital video broadcasting (DVB).

1.3.4.9. 5G

The ITU specification for 5G represents a radical change in performance compared with 4G and aims to meet the requirements of emerging applications, described above. Data rates of up to 10 Gbit/s (100 times faster than 4G networks) aim to satisfy the growing demand for bandwidth; latencies of 1mSec (30- 50mSec for 4G) will enable near real-time response rates; and connection densities of 1,000 devices per square kilometer (100 times more than 4G) will support the growing number of IoT devices and sensors.

Chapter 02 : Access protocols and QoS in WLANs

2.1. Introduction

A wireless local area network (WLAN) is a wireless distribution method for two or more devices. WLANs use high-frequency radio waves and often include an Internet access point. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection. In this chapter we'll look at the different access protocols in WLANs, as well as quality of service in this type of network.

2.2. WLAN applications

Wireless LANs have many real-world applications. They are frequently used to enhance a wired network, not to replace it completely. The following sections describe some of the applications made possible by the power and flexibility of wireless LAN technology.

2.2.1. Healthcare sector

Doctors and nurses equipped with laptops have faster access to patient data. What's more, in the event of an emergency, they can communicate with other hospital departments using WLAN to provide rapid diagnoses.

2.2.2. Day-to-day business

In business, people can work productively with customers or suppliers in meeting rooms - there's no need to leave the room to check if important e-mails have arrived or print out large files. Instead, you can send them from one laptop to another.

2.2.3. In-building network managers

Network managers in older buildings, such as schools, hospitals and warehouses, find WLANs to be the most cost-effective infrastructure solution. When building a new network or extending the old internal network, little or no cable needs to be run through walls and ceilings.

2.2.4. Network operators in dynamic environments

Network managers in dynamic environments minimize the cost of moves, network extensions and other modifications by eliminating cabling and installation costs. The

mobile nature of WLAN means that a new network can be built and tested before moving to a critical environment.

2.3. WLAN access protocols

WLAN technology in the IEEE 802.11 standard covers the "Network Access" layer of the TCP/IP model, or the "Physical" (L1) and "Data Link" (L2) layers of the OSI model. The IEEE 802.11 Wi-Fi standard aims to avoid collisions with CSMA/CA for "Collision Avoidance" on a shared medium such as air, using contention mechanisms. But there are also other techniques, such as TDMA for Time Division Multiple Access.

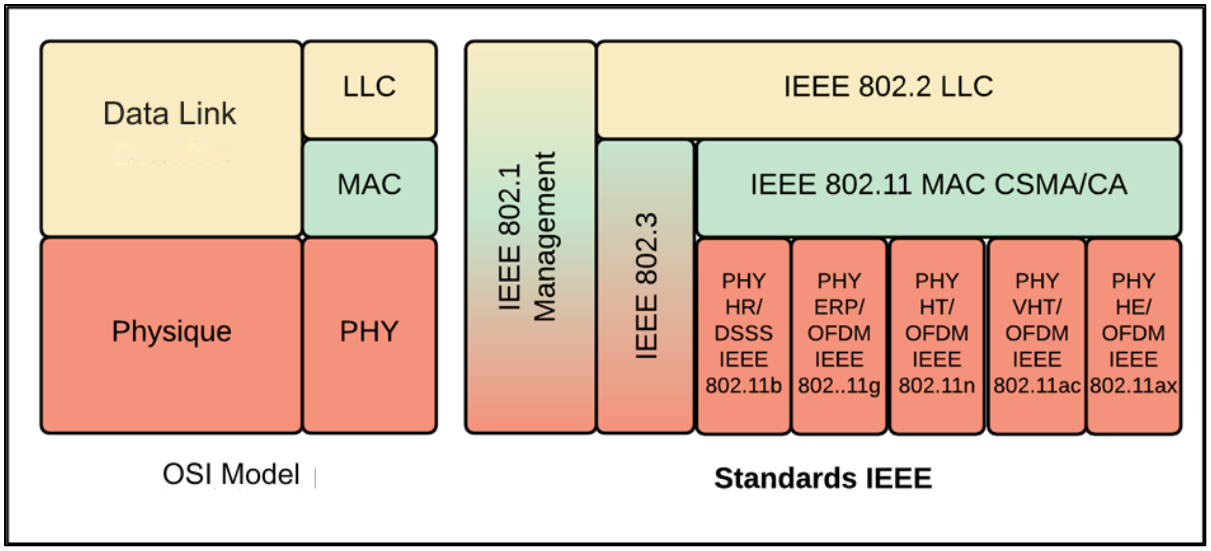


Figure 2.1. IEEE 802.11 Access Layer

The data link layer is responsible for transmitting data between two nodes. Its main functions are:

- Data link control
- Multiple access control

2.3.1. Data link control

Data link control is responsible for the reliable transmission of the message on the transmission channel, using techniques such as screening, error control and flow control.

2.3.2. Multiple access control

If there is a dedicated link between sender and receiver, the data link control layer is sufficient, but if there is no dedicated link, several stations can access the channel simultaneously. Consequently, several access protocols are needed to reduce collisions and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a

question and all the students (or stations) start answering simultaneously (sending data at the same time), then a lot of chaos is created (overlapping or loss of data) so it's the teacher's job (multiple access protocols) to manage the students and get them to answer one by one. Protocols are needed to share data over non-dedicated channels. Several access protocols can be subdivided as illustrated in the following figure:

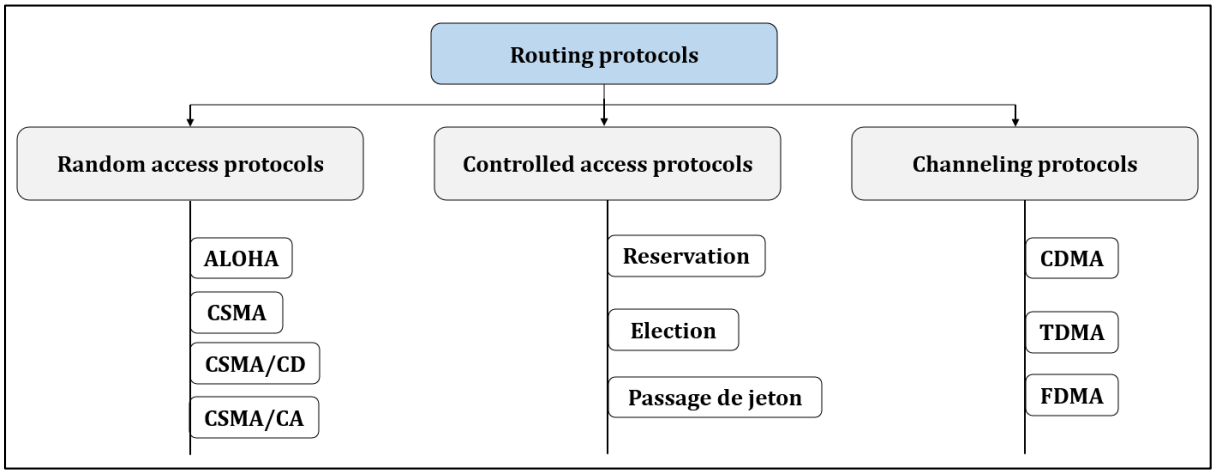


Figure 2.2. Multiple access protocols

2.3.2.1. Random access protocol

All stations have the same superiority, i.e., no station has a higher priority than another. Any station can send data depending on the state of the medium (idle or busy). It has two features:

- There is no fixed time for sending data.
- There is no fixed sequence of stations sending data.

2.3.2.2. Controlled access protocols

In controlled access, stations inform each other to find out which station has the right to transmit. It allows only one node to send at a time, to avoid collision of messages on the shared medium. The three methods of controlled access are: reservation, election and token passing.

2.3.2.3. Channeling

In this, the available bandwidth of the link is shared in time, frequency and code with several stations to access the channel simultaneously.

2.3.2.4. ALOHA protocol

This protocol was designed for wireless LANs, but also applies to shared media. In this case, several stations can transmit data at the same time, leading to collisions and scrambled data.

- **Aloha pure:** When a station sends data, it waits for an acknowledgement. If the acknowledgement doesn't arrive within the allotted time, the station waits for a random period of time called waiting time and sends the data back. As different stations wait for different times, the probability of new collisions decreases.
- **Slot Aloha:** This is similar to pure Aloha, except that we divide the time into slots and only allow data to be sent at the start of these slots. If a station misses the allotted time, it has to wait for the next slot. This reduces the probability of collision.

2.3.2.5. CSMA protocol

Carrier Sense Multiple Access guarantees fewer collisions, as the station must first detect the medium (idle or busy) before transmitting data. If it is idle, it sends data, otherwise it waits for the channel to become idle. However, there is always a risk of collision in CSMA due to the propagation delay. For example, if station A wants to send data, it will first detect the medium. If it finds the channel inactive, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and detects the medium, it will also find it inactive and will also send data. This will result in a data collision between stations A and B.

2.3.2.6. CSMA/CA protocol

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a network protocol that avoids a collision rather than allowing it to occur, and does not deal with packet recovery after a collision. It is similar to the CSMA/CD protocol, which operates at the media access control layer. In CSMA/CA, every time a station sends a data frame to a channel, it checks to see if it's in use. If the shared channel is busy, the station waits for the channel to switch to idle mode. As a result, we can say that it reduces the risk of collisions and makes better use of the medium to send data packets more efficiently. This protocol is used in 802.11 networks (a set of standards for local wireless networks).

CSMA/CA avoids collisions by:

- **Interframe space:** The station waits for the medium to become inactive, and if it is found to be inactive, it doesn't immediately send data (to avoid a collision due to propagation delay), but waits for a period called interframe space or IFS. After this time, it checks again whether the medium is inactive. The IFS time depends on the station's priority.
- **Contention window:** This is the duration divided into slots. If the sender is ready to send data, he chooses a random number of slots as the wait time, which doubles every time the medium is not found to be idle. If the medium is found to be busy, it does not restart the whole process, but rather the timer when the channel is found to be inactive again.
- **Acknowledgement:** The sender retransmits data if the acknowledgement is not received before the timer expires.

The advantages of CMSA/CA:

- CMSA/CA prevents collisions.
- Thanks to acknowledgements, data is not lost unnecessarily.
- This avoids unnecessary transmissions.
- It is ideally suited to wireless transmission.

Limitations of CSMA/CA:

- The algorithm requires long waiting times.
- High power consumption.

2.3.2.6.1. Operations

- When a frame is ready, the transmitting station checks whether the channel is free or busy.
- If the channel is busy, the station waits for the channel to become inactive.
- If the channel is idle, the station waits for a time interval between frames and then sends the frame.
- After sending the frame, it sets a timer.
- The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before the timer expires, it marks a successful transmission.
- Otherwise, it waits for a delay period and restarts the algorithm.

2.3.2.6.2. Types of media access

DCF (Distributed coordination function) and PCF (Point coordination function) are two types of 802.11 bearer access. They are the mechanisms for implementing CSMA/CA in the wireless LAN.

DCF is the basis of the CSMA/CA protocol access mechanism. Like Ethernet, it first checks that the radio link is free before transmitting. To avoid collisions, stations use a random backoff (interrupt) after each frame, with the first transmitter seizing the channel.

In PCF, coordinators are used to ensure that the medium is provided without contention. Point coordinators reside in access points, so PCF is limited to infrastructure networks. To gain priority over standard contention-based services, PCF allows stations to transmit frames after a shorter interval. PCF is not widely implemented.

2.4. QoS in WLAN networks

Quality of Service (QoS) is the use of mechanisms or technologies that operate on a network to control traffic and ensure the performance of critical applications with limited network capacity. It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.

QoS is generally applied to networks carrying traffic for resource-intensive systems. Common services for which it is required include Internet protocol television (IPTV), online gaming, streaming media, videoconferencing, video-on-demand (VOD) and voice over IP (VoIP).

QoS is integrated into Wi-Fi technology with the adoption of the IEEE 802.11e standard. The 802.11e standard includes two modes of operation, each of which can be used to improve service for voice:

- Wi-Fi Multimedia Extensions (WME) - Mandatory
- Wi-Fi Programmed Multimedia (WSM) - Optional

2.4.1. QoS privileges

Deploying QoS is crucial for companies wishing to ensure the availability of their critical applications. It is essential for providing differentiated bandwidth and ensuring that data transmission takes place without interrupting traffic flow or causing packet loss. Key benefits of QoS deployment include:

- **Unlimited application prioritization:** QoS ensures that business-critical applications always have the priority and resources they need to achieve high performance.
- **Better resource management:** QoS enables administrators to better manage the organization's Internet resources. This also reduces costs and the need to invest in link extensions.
- **Enhanced user experience:** The ultimate aim of QoS is to guarantee high performance for critical applications, which means delivering an optimal user experience. Employees benefit from high performance on their high-bandwidth applications, enabling them to be more efficient and get their work done faster.
- **Point-to-point traffic management:** network management is vital, no matter how traffic is routed, whether end-to-end, node-to-node or point-to-point. The latter enables organizations to deliver client packets in sequence from point to point on the Internet without suffering packet loss.
- **Packet loss prevention:** packet loss can occur when data packets are dropped in transit between networks. This can often be caused by an outage or inefficiency, network congestion, a faulty router, a loose connection or a poor signal. QoS avoids the potential for packet loss by prioritizing bandwidth for high-performance applications.
- **Latency reduction**: latency is the time it takes for a network request to pass from sender to receiver, and for the receiver to process it. This is generally affected by routers taking longer to analyze information and storage delays caused by intermediate switches and bridges. QoS enables organizations to reduce latency or speed up the process of a network request by giving priority to their critical application.

2.4.2. How does QoS work?

QoS networking technology works by marking packets to identify service types, then configuring routers to create separate virtual queues for each application, according to their priority. As a result, bandwidth is reserved for critical applications or websites to which priority access has been assigned.

QoS technologies provide an allocation of capacity and processing to specific flows in network traffic. This enables the network administrator to assign the order in which packets are processed, and provide the appropriate amount of bandwidth to each application or traffic flow.

2.4.3. QoS metrics

They are used to quantitatively measure the quality of service of a network; QoS metrics refer to objective, system-related characteristics that provide insight into the performance of the delivery service.

2.4.3.1. Bandwidth

The maximum amount of data transmitted over an Internet connection in a given time. For example, allocating a certain amount of bandwidth to different queues for different types of traffic.

2.4.3.2. Delay

This is the time taken for a packet to pass from its source to its final destination. This can often be affected by queuing delay, which occurs during periods of congestion when a packet waits in a queue before being transmitted. QoS enables organizations to avoid this by creating a priority queue for certain types of traffic.

2.4.3.3. Date loss

The amount of data lost as a result of packet loss, usually due to network congestion. QoS allows organizations to decide which packets to drop in this event.

2.4.3.4. Jitter

Change in the time taken for a data packet to travel across a network. Data packets get stuck on their way to the receiver, usually because the network is congested. They will arrive at irregular intervals, which can lead to distortion or gaps in audio and video broadcasting.

2.4.4. Techniques involved in QoS

There are several techniques that companies can use to guarantee high performance for their most critical applications.

2.4.4.1. Prioritization of delay-sensitive VoIP traffic via routers and switches

Many corporate networks can become too congested, causing routers and switches to start dropping packets as they flow in and out faster than they can be processed. As a result, streaming applications suffer. Prioritization allows traffic to be classified and given different priorities according to its type and destination. This is particularly useful in a situation of heavy congestion, as packets with a higher priority can be sent before the rest of the traffic.

2.4.4.2. Resource reservation

Resource Reservation Protocol (RSVP) is a transport-layer protocol that reserves resources on a network and can be used to provide specific levels of QoS for application data flows. Resource reservation enables companies to divide network resources by traffic of different types and origins, define limits and guarantee bandwidth.

2.4.4.3. Queuing

Queuing is the process of creating policies that give preferential treatment to certain data flows over others. Queues are high-performance memory buffers in routers and switches, in which transiting packets are held in dedicated memory areas. When a packet is assigned a higher priority, it is moved to a dedicated queue that pushes data through at a faster rate, reducing the risk of it being dropped. For example, companies can assign a strategy to prioritize voice traffic over the majority of network bandwidth. The routing or switching device will then move packets and frames of this traffic to the front of the queue and transmit them immediately.

2.4.4.4. Traffic marking

When applications requiring priority over other bandwidth other bandwidth on a network have been identified, the traffic must be marked. This is made possible by processes such as class of service (CoS), which marks a data stream in the Layer 2 frame header, and the differentiated services code point (DSCP), which marks a data stream in the in the Layer 3 packet header.

2.4.5. The 802.11e standard

The 802.11e standard will include two modes of operation, each of which can be used to enhance the service for voice:

- Wi-Fi Multimedia Extensions (WME) - Mandatory
- Wi-Fi Programmed Multimedia (WSM) - Optional

2.4.5.1. Wi-Fi Multimedia Extensions (WME)

Wi-Fi Multimedia Extensions use a protocol called Enhanced Multimedia Distributed Control Access (EDCA), which is an extension of an enhanced version of the Distributed Control Function (DCF) defined in the original 802.11 MAC.

The enhanced part is that EDCA will define eight levels of priority for access to the shared wireless channel. Like the original DCF, EDCA access is a contention-based protocol that uses a set of wait intervals and wait timers designed to avoid collisions. However, with DCF, all stations use the same values and therefore have the same transmission priority on the channel. With EDCA, each of the different access priorities is assigned a different range of wait intervals and wait counters. Transmissions with a higher access priority are assigned shorter intervals. The standard also includes a packet burst mode that allows an access point or mobile station to reserve the channel and send 3 to 5 packets in sequence.

2.4.5.2. Wi-Fi Scheduled Multimedia (WSM)

Consistent delay services can be provided with the optional Wi-Fi Scheduled Multimedia (WSM). WSM works like the little-used Point Control Function (PCF) defined with the original 802.11 MAC.

In WSM, the access point periodically broadcasts a control message that forces all stations to treat the channel as busy and not attempt to transmit. During this period, the access point polls each station defined for a time-sensitive service. To use the WSM option, devices must send a traffic profile describing bandwidth, latency and jitter requirements. If the access point does not have sufficient resources to meet the traffic profile, it will return a busy signal.

2.4.6. QoS at Layer 3

When a device is running Lightweight Access Point Protocol (LWAPP), packets to the host router are encapsulated in a Layer 3 LWAPP header with the IP DSCP field set to one of the values shown in the table below, depending on the type of traffic.

Table 2.1. LWAPP packets and QoS marking

Cisco AVVID 802.1pUP-Based Traffic Type	**Cisco AVVID IP DSCP**	**Cisco AVVID 802.1p UP**	**IEEE 802.11e UP**	**Notes**
Network control	-	7	-	Reserved for network control only
Inter-network control	48	6	7 (AC_VO)	Control LWAPP
Voice	46 (EF)	5	6 (AC_VO)	Controller: Platinum QoS profile
Video	34 (AF41)	4	5 (AC_VI)	Controller: Gold QoS profile
Voice control	26 (AF31)	3	4 (AC_VI)	-
Best effort	0 (BE)	0	3 (AC_BE)	

Chapter 03 : Ad hoc networks: MANET

3.1. Introduction

An Ad Hoc network is a set of entities interconnected by wireless technology, forming a temporary network without the aid of any administration or fixed support. This new environment offers many advantages over the usual environment. However, new problems may arise, caused by the new system characteristics: the routing problem is far from obvious in mobile networks, and particularly in Ad Hoc networks.

Ad hoc networks are characterized by their lack of administration and there are no fixed elements in an Ad Hoc network. In an Ad Hoc network, all the elements must cooperate to create a temporary architecture for communications. To create this architecture for routing data, Ad Hoc networks must use high-performance routing protocols. This chapter introduces the basic concepts of Ad Hoc networks, such as routing and quality of service.

3.2. Definition: mobile ad hoc networks

A mobile ad hoc network, usually referred to as MANET (Mobile Ad hoc Network), consists of a large, relatively dense population of mobile units moving around any given territory, whose only means of communication is via wireless interfaces, without the aid of any pre-existing infrastructure or centralized administration. Figure 3.1 shows an example of the topology of nodes forming an ad hoc network.

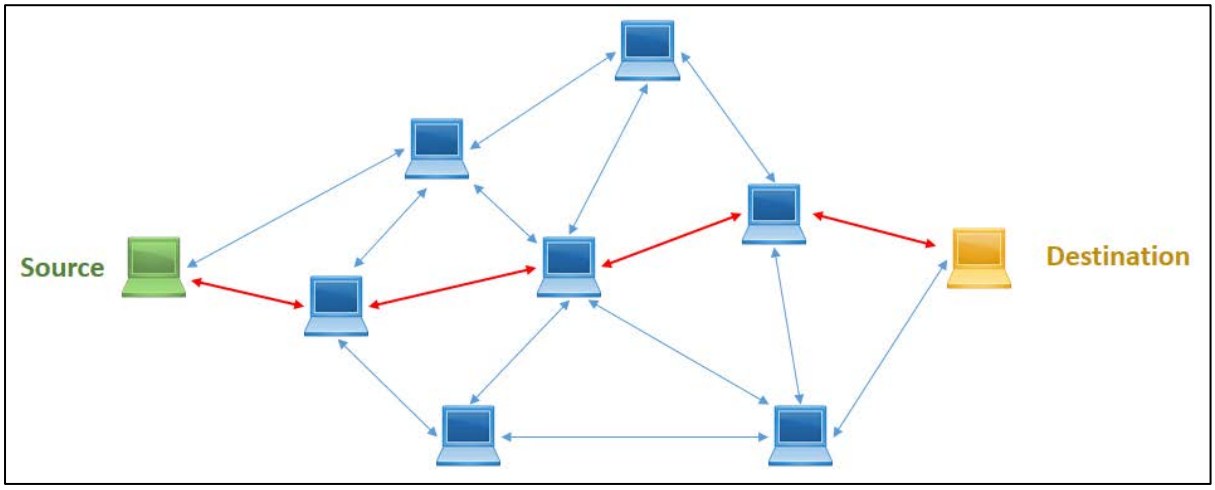


Figure 3.1. Ad hoc network

3.3. Characteristics

All the characteristics of a wireless communication network are applicable to Mobile Ad Hoc networks, although there are certain properties that are specific to this type of network:

- **Mobility of all nodes (dynamic topology):**

This is an intrinsic feature of MANETs. Moving nodes causes random, unpredictable changes to the network architecture.

- **Equivalence of network nodes:**

In a conventional network, there is a clear distinction between end nodes (stations, hosts) and internal nodes (routers, for example) in the network. This difference does not exist in ad hoc networks, as all nodes may be required to perform routing functions.

- **Limited physical security:**

Ad hoc networks generally have a low level of physical security, due to the use of radio media. There are greater opportunities for intruders to infiltrate the network, detection of an intrusion or denial of service is more delicate, and the lack of centralization makes gathering information for intrusion detection more complex.

- **Limited bandwidth:**

A key feature of wireless networks is the use of a shared communication medium. This sharing means that the bandwidth reserved for a host is modest.

- **Multi-hop communications:**

In a MANET, nodes that can't reach destination nodes directly will need to relay their data via other nodes.

- **No infrastructure:**

Ad hoc mobile networks are distinguished from other mobile networks by the property of absence of pre-existing infrastructure and any kind of centralized administration.

- **Energy constraints:**

Mobile hosts are powered by autonomous energy sources such as batteries or other consumables. The energy parameter must be taken into account in any control performed by the system.

3.4. Routing in MANETs

Routing is a method of routing information to the right destination through a given connection network. It consists in providing a strategy that guarantees, at any given time, the establishment of correct and efficient paths between any pair of nodes belonging to the network, thus ensuring the continuous exchange of messages. Given the limitations of Ad hoc networks, path construction must be carried out with a minimum of control and bandwidth consumption.

3.4.1. Classification of routing protocols

Depending on the way in which paths are created and maintained during data routing, routing protocols can be separated into three categories: proactive protocols, reactive protocols and hybrid protocols. The figure below shows the typology of the main routing protocols in ad hoc networks.

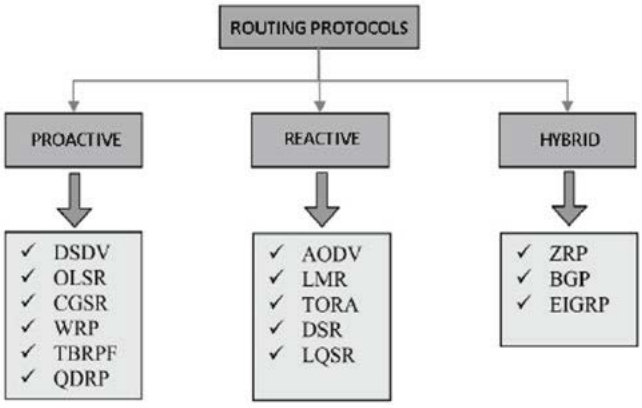


Figure 3.2. Classification of routing protocols in ad hoc networks

3.4.1.1. Proactive routing protocols

A proactive routing protocol maintains regularly updated information on the network topology at each node, enabling each mobile to quickly know a path to each destination in the network. The two main methods used are the "Link State" method and the "Distance Vector" method. Both require periodic updates of routing data, which must be broadcast by the network's various routing nodes. These protocols are "table-driven", meaning that each node uses its own routing table to route data to a specific neighbor until it reaches the desired destination. The performance of proactive routing is characterized by:

- Lowest latencies, since applications wishing to transmit can assume the existence of up-to-date, valid paths.
- High energy consumption and high bandwidth usage, due to the fact that the path update protocol is constantly in use, even if the paths are never used.

The most important protocols in proactive routing are OLSR and DSDV.

3.4.1.2. Reactive routing protocols

Reactive routing operates on demand. No information is stored in routers about destinations to which the node concerned has no active path.

When an application wishes to contact a correspondent, and only then, a path is searched according to the request-response principle. When a node wants to initiate communication with another node, it starts a path discovery process. Once the path has been found, it is maintained by a path maintenance procedure, until the path is no longer in use. This type of protocol has the advantage of not overloading the network with control traffic, and of requiring only minimal router storage capacity. However, it can take a long time to establish communications when the network is busy, or when the correspondent is a long way from the sender. The most widely used protocols in this family are AODV, DSR and TORA.

3.4.1.3. Hybrid routing protocols

Hybrid protocols combine the two ideas or techniques of proactive and reactive protocols. They use the principle of proactive protocols to obtain information about the nearest neighbors (maximum two-hop neighbors). Beyond this predefined zone, the hybrid protocol uses reactive protocol techniques to search for paths.

This type of protocol is a solution that combines the advantages and disadvantages of the two previous approaches, using a notion of Ad Hoc mobile network slicing. Several hybrid protocols exist, such as ZRP.

3.4.2. The AODV protocol

AODV (Ad hoc On Demand Distance Vector) is a reactive routing protocol, using a path discovery mechanism inspired by DSR and DSDV. Once the path has been traced, nodes that are not on the active path do not maintain any routing information and do not participate in any update exchanges. Because of the mobility of nodes in ad hoc networks, paths change frequently, so that paths maintained by some nodes become invalid. Sequence numbers enable the use of the newest or freshest routes, to force updates when necessary and avoid routing loops. Paths are established and maintained by exchanging various types of messages:

- **RREQ: Route Request Message**, broadcast to all neighboring nodes by a source wishing to send data packets to a destination.

Table 3.1. Format of an RREQ

@Source	**Num. seq. Source**	**Broadcast id**	**@Destination**	**Num. seq. Destination**	**Number of hops**

- **RREP: "Route Reply Message",** once the destination receives the RREQ, it replies with an RREP as an acknowledgement of receipt, the reverse path of RREQ.

Table 3.2. Format of an RREP

@Source	***@Destination***	***Num. seq. Destination***	**Number of hops**	***Life time***

- **Hello message: "Are you there?",** message broadcast periodically to the immediately neighboring node to see if it's still there; if there's no Hello message arriving from a particular node, the neighbor assumes that this node has moved and marks this link as interrupted.

Table 3.3. Format of HELLO message

@source	**Num. seq. Source**	**Number of hops**	**Life time**

- **RERR: "Cancel route",** message sent by a node when it detects that the link with its neighbor is broken (invalid path).

Table 3.4. Format of an RERR

Destination @ List	Destination Num. seq. List	Number of destinations @

With:

- @Source: source node address.
- @Destination: destination node address.
- Num. seq: sequence number.
- Life time: message lifetime.
- Broadcast ID: Broadcast identifier for messages sent.
- NB hops: number of hops.

AODV's routing table management maintains paths in a distributed way, by keeping a routing table at each intermediate node belonging to the path being searched. Each routing table entry contains the following fields:

- Destination node address: this is the IP address of the destination node to be reached.
- Next node address: the IP address of the node to which a packet is to be routed to reach a destination.
- Number of hops separating the source node from the destination node
- Sequence number associated with the destination,
- Lifetime for which the path remains available to the source node.
- List of neighbors using this path: IP addresses of any precursor nodes used by the current node as a next hop to reach the destination.

3.4.2.1.1. How AODV operates?

The AODV protocol defines two types of operation: path discovery and path maintenance. AODV does not use periodic updates; paths are discovered and maintained as required.

Path discovery:

The path discovery mechanism is the process of searching for a path at the request of source nodes. When a source node "S" wishes to establish a path to a destination "D" for which it does not yet have a path, it broadcasts a Route Request (RREQ) packet across the network. The nodes receiving the packet establish pointers back to the source in the routing tables.

Next, it checks whether it has received the same request before, in which case it "silently" destroys (without announcing this operation to the other nodes) the received packet. If the request has not been received before, the node increments the number of hops in the packet and rebroadcasts it. At the same time, the intermediate node creates an entry in its routing table pointing to the source node: this is the reverse path, as shown in Figure 3.3. This path will later be used for the eventual transmission of RREP messages to the source node.

If the node receiving the RREQ has no path to the destination, it rebroadcasts the RREQ and creates a reverse path to the source IP address. Otherwise, it generates a Route Reply (RREP) message to the source.

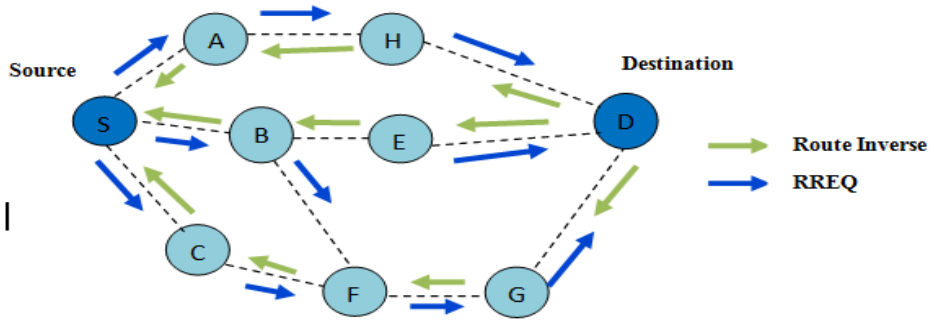


Figure 3.3. Broadcasting RREQ packet: reverse path creation

Route Reply (RREP) message generation:

A node generates a Route Reply (RREP) message in two cases:

- It is the destination

- It has in its routing table a route to the destination whose sequence number is greater than or equal to the sequence number in the RREQ message received.

Then, the RREP message is sent to the source following the same arrival path. If the source is an intermediate node, it adds the distance separating it from the destination to the RREP message. (Figure 3.4)

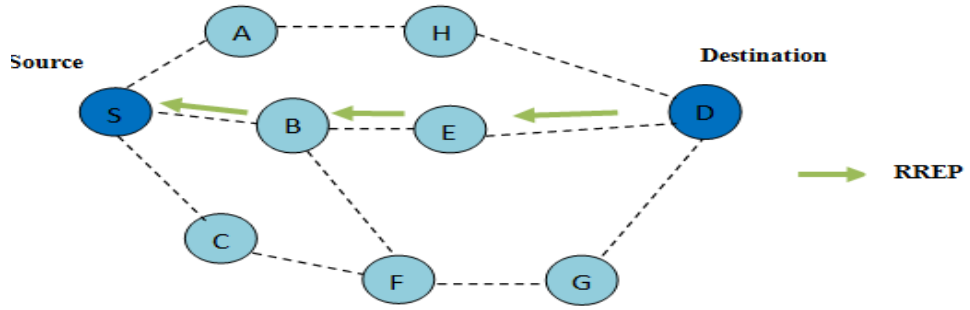


Figure 3.4. RREP response to the source node

Path maintenance and connectivity management

As soon as a path is established between a source node and a destination, a maintenance mechanism is automatically triggered. This mechanism essentially handles connectivity management, i.e., how to detect a failure and how to remedy it.

Each node on an active path must periodically check the link status with the successor node on the same path. This is done by broadcasting the "HELLO" message, with the broadcast period set to a duration of "HELLO_INTERVAL" (in MS). This message is nothing more than a RREP containing the sender's address with a TTL equal to 1 to prevent it from being propagated further in the network.

Thus, if a node does not receive a HELLO message from a neighboring node during a period that is a multiple of "HELLO_INTERVAL", we conclude that the link with this node is broken, and therefore there is a change in neighboring connectivity.

Link failures are generally due to node mobility:

If the source node moves and breaks the link with its successor, then it will restart the path establishment procedure if it still needs to.

If the node that has moved is an intermediate or destination node, then the source node must be informed by the RERR message, which must be generated by the nearest of the two nodes (Figure 3.5). The RERR initiator will list its precursor nodes on the failed path and send them the RERR packet. On receiving a RERR, a node marks the path to this

invalid destination (whose address appears in the RERR) by setting the value of the corresponding distance field to infinity (Distance = infinite), and in turn forwards the RERR to its precursors on this path. When the source node receives the RERR, it starts a new process to establish a new path if it still needs one.

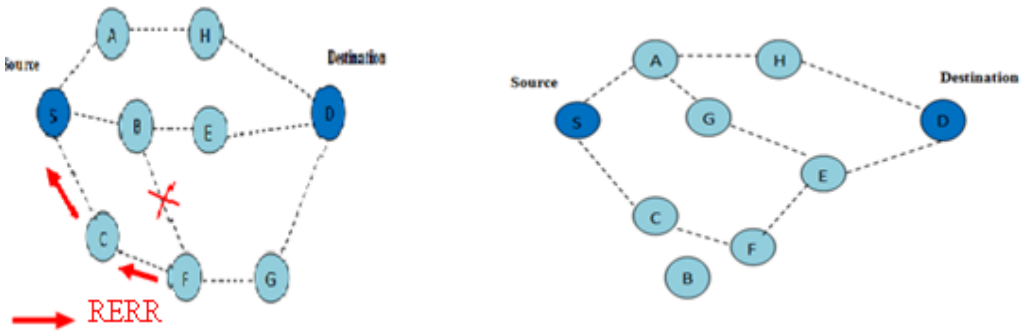


Figure 3.5. RERR generation due to node B failure

In short, AODV broadcasts a path request for each unknown destination in restricted flooding, to which any station that knows how to reach the destination responds. The fastest response allows each intermediate node to define which neighbor to use to reach the destination.

3.5. QoS in ad hoc networks

The main objective of QoS-based routing is to find the path through the network, providing sufficient resources to meet QoS requirements. Common QoS requirements for real traffic are maximum delay threshold, minimum bandwidth threshold and constant jitter. The problem of finding the route with two or more QoS metrics in MANETs is NP-complete. This makes it very difficult to design and implement a routing protocol that can be optimal in every situation. This section describes some of the most widely used routing protocols designed to support QoS in MANETs.

3.5.1. CEDAR

Core Extraction Distributed Ad Hoc Routing (CEDAR) is a routing protocol that dynamically establishes the network core, then propagates stable, high-bandwidth link states to the core nodes. Route selection and calculation is on-demand, and is performed by the route nodes using only their local state information. This routing protocol consists of three components: core extraction, link state propagation and route calculation. Core

extraction means electing certain nodes, which are then responsible for maintaining the topology and calculating the path for their domain.

3.5.2. QoS AODV

The ad hoc distance vector on demand (AODV) routing protocol has been extended to support quality of service. It includes object extension on Route Request (RREQ) and Route Reply (RREP) messages, which specify bandwidth or delay parameters during the route discovery phase. A node becomes a hop on the route only if it can meet the requirements specified in the RREQ. If the route has already been established and the specified QoS requirement can no longer be met, the node sends an ICMP QOS_LOST message to the source node.

3.5.3. Bandwidth routing

The Bandwidth routing (BR) protocol works solely with bandwidth as a QoS metric. The best path is the shortest path satisfying bandwidth requirements. The entire protocol consists of an end-to-end path bandwidth calculation algorithm, a bandwidth reservation and a backup routing algorithm to restore QoS flow in the event of a path break.

3.5.4. On-Demand QoS Routing

The On-Demand QoS Routing (OQR) protocol is very similar to BR, but the network is temporal. Unlike BR, it is not a hybrid, but a typical representative of reactive protocols. Route discovery is therefore an important component. Another component is admission control, which guarantees bandwidth for real-time applications.

Chapter 04 : Wireless sensor networks

4.1. Introduction

Today, sensors are everywhere. We take it for granted, but sensors are in our phones, our workplaces, our vehicles and our environment. A sensor network comprises a group of small, powered devices and a wireless or wired network infrastructure. They record conditions in a number of environments, including industrial facilities, farms and hospitals. The sensor network connects to the Internet or computer networks to transfer data for analysis and use. Sensor network nodes detect and control the environment cooperatively. They enable interaction between people or computers and the surrounding environment. This chapter introduces the main applications of sensor networks, then focuses on the study of the Mac layer and routing in this type of network. Finally, it examines the different strategies for managing energy and security in sensor networks.

4.2. Definition: Wireless sensor networks

Wireless Sensor Networks (WSNs) have the power of distributed communication, computing and sensing functionalities. They are characterized as infrastructure-free, fault-tolerant and self-organizing networks that offer low-cost, easy-to-apply, fast and flexible installation possibilities in an environment for a variety of applications.

Among the characteristics of wireless capture networks:

Resource constraints: WSN nodes are smaller and battery-powered. This means that the service provided by the nodes, such as communication and computing memory, is very limited.

Communication paradigm: WSN's data-centric functionality explains its data-centric nature and justifies that communication is limited to the nodes.

Application-specific design: WSN is application-specific, i.e., the architecture of WSN is based on the application.

Node failure and unreliable communication: Various factors such as harsh operating conditions leading to instability, unpredictability, nodal mobility and environmental interference make typical WSN nodes prone to errors.

Scalability and density: The number of nodes in WSNs can be large and densely deployed to a greater degree in various applications.

Dynamic topologies: Nodes are free to move randomly at different speeds in some applications, and can sometimes fail, be added or replaced. This can result in a different network topology.

Communication models: WSNs use different communication models - flat/hierarchical/distributed WSNs; or homogeneous/heterogeneous WSNs..

4.3. Main applications

Among the fields of application for sensor networks we have the following:

- Internet of Things (IoT)
- Security surveillance, threat detection
- Ambient temperature, humidity and atmospheric pressure
- Environmental noise levels
- Medical applications such as patient monitoring
- Agricultural applications
- Landslide detection
- Intelligent parking and lighting

4.4. WSN components

Sensors:

WSN sensors are used to capture environmental variables and are used for data acquisition. Sensor signals are converted into electrical signals.

Radio nodes:

This is used to receive the data produced by the sensors and send it to the WLAN access point. It consists of a microcontroller, transceiver, external memory and power source.

Wi-Fi access point:

It receives data sent by wireless radio nodes, usually via the Internet.

Evaluation software:

The data received by the WLAN access point is processed by software called evaluation software to present the report to users for further processing of the data, which can be used for data processing, analysis, storage and exploration.

4.5. Sensor node architecture

Depending on the type of application, there are a variety of sensors that can be grouped into three classes: optical sensors, thermal sensors and mechanical sensors. A hardware architecture applicable to most intelligent sensors is shown in Figure 4.1.

A sensor contains four basic units: the sensing unit, the processing unit, the transmission unit and the energy control unit. Depending on the application, additional modules can be added, such as a positioning system (GPS), or an energy-generating system (solar cell). Some larger micro-sensors are equipped with a mobilizing system to move them if necessary.

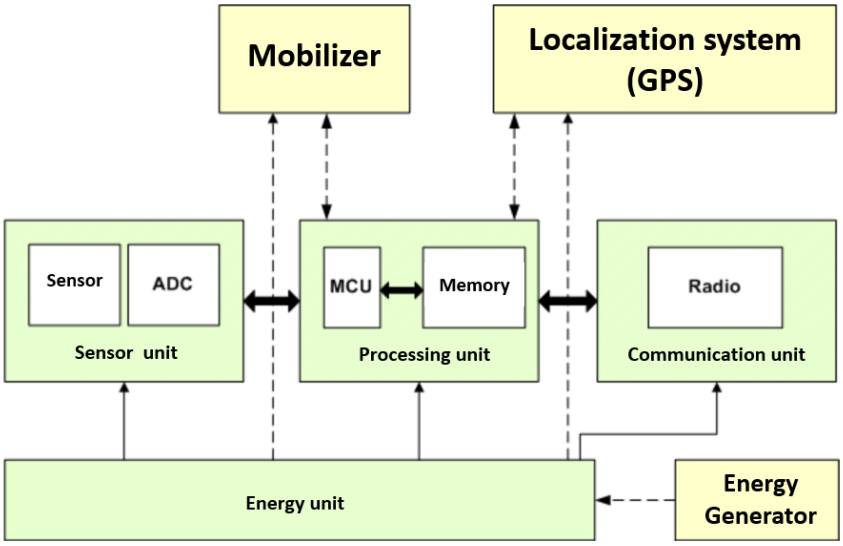


Figure 4.1. Sensor architecture

Sensor unit:

This is the unit responsible for capturing physical quantities (heat, humidity, vibrations, radiation, etc.) and transforming them into digital quantities (an electrical signal). This unit can incorporate from one to several sensors plus an ADC unit (Analog to Digital Converters). The latter's role is to convert the analog signal produced by the sensors, which is based on the sampled data, into a digital signal that can be understood by the processing unit.

Processing unit:

The processing unit can be considered as the intelligent part of the sensor. It includes a processor, usually associated with a small storage unit. It manages programs and software, stores metrological and functional parameters in memory (dated by the internal clock), and processes data received from the sensor unit. The processing unit generally controls the other units. The processors used in sensor networks have low power consumption and low frequency. Storage memory is also very limited, on the order of 10KB of RAM for data and 10KB of ROM for programs. This memory consumes most of the processing unit's energy. In most cases, it is supplemented by a less energy-intensive flash memory.

Communication unit:

This unit provides the connection between network nodes. A radio module (transmitter/receiver) is integrated into this unit, enabling communication between different network nodes. Communication can be optical or radio frequency. It is responsible for the transmission-reception of captured and processed data via a wireless communication channel. The radio module consumes the most energy.

Energy unit:

For sensor networks, the energy unit is the most important component, usually a battery. This battery is small and has limited energy capacity. Sensors are often located in hostile environments, inaccessible to human beings, and the battery is generally not replaceable. In such situations, it is virtually impossible to recharge or replace the battery. For this reason, energy is the main constraint when designing a wireless sensor network, since it influences the lifetime of the sensor node and therefore the lifetime of the network. However, it is possible to use systems for recharging energy from the environment via photovoltaic cells, for example, to extend battery life.

Complement:

Depending on the needs of the sensor network application, the sensor node can integrate other units such as:

Location system: to determine the node's position.

Mobilizer: to change the node's position.

4.6. Design challenges in WSNs

There are major design challenges in wireless sensor networks due to the lack of resources such as energy, bandwidth and processing storage. When designing new routing protocols, the following essential elements must be fulfilled by a network engineer.

4.6.1. Energy efficiency

Wireless sensor networks are mainly battery-powered. Energy scarcity is a major problem in these sensor networks, particularly in aggressive environments such as battlefields, etc. Sensor node performance is affected when the battery falls below a predefined battery threshold level. Energy presents a major challenge for designers when designing sensor networks. In the wireless sensor network, there are millions of particles. Each node in this network has limited energy resources due to a partial amount of power. So, the routing protocol must be energy-efficient.

4.6.2. Complexity

The complexity of a routing protocol can affect the performance of the entire wireless network. The reason is that we have insufficient hardware skills, and we also face extreme energy limitations in wireless sensor networks.

4.6.3. Scalability

As sensors become cheaper by the day, hundreds or even thousands of sensors can be easily installed in a wireless sensor network. The routing protocol must therefore support network scalability. If further nodes are to be added to the network at any time, the routing protocol must not interrupt this.

4.6.4. Delay

Some applications require an instant reaction or response without substantial delay, such as a temperature sensor or alarm monitoring, etc. The routing protocol must therefore not interrupt this. The routing protocol must therefore offer a minimum delay. The time required to transmit the detected data should be as short as possible.

4.6.5. Robustness

Wireless sensor networks are deployed in very critical environments, where losses are frequent. Sometimes, a sensor node may expire or leave the wireless sensor network. So

the routing protocol must be able to cope with all kinds of environments, including severe and lossy ones. The functionality of the routing protocol should also be good.

4.6.6. Data transmission and transmission models

There are four modes of data transmission depending on the applications in wireless sensor networks, namely query-driven, event-driven, continuous and hybrid. A node starts transmitting data only when the receiver creates the request or an event occurs in both the request-driven and event-driven models. Data is sent periodically in continuous transmission mode. The performance of the routing protocol depends on the size of the network and the transmission media. A good quality transmission medium directly improves network performance.

4.6.7. Sensor location

Another major challenge facing designers of wireless sensor networks is locating sensor nodes correctly. Most routing protocols use a localization technique to obtain information about their locations. Global Positioning System (GPS) receivers are used in some scenarios.

4.7. MAC layer studies for sensor networks

The MAC layer is responsible for establishing a reliable and efficient communication link between WSN nodes, and for wasting energy.

There are different types of MAC protocols, which can be classified into two categories as CSMA/CA (carrier sense multiple access with collision avoidance) and TDMA (time division multiple access). CSMA/CA protocols are based on Carrier Sense Multiple Access (CSMA), which is a probabilistic technique where each node listens (carrier sense) before sending, and if no one transmits, the node will try to transmit a packet. The term multiple access means that several sensor nodes can access the medium at the same time, and simultaneous transmission causes a collision which must be resolved by a technique such as Binary Exponential Backoff (BEB). Unlike collision-based protocols, TDMA protocols are known as deterministic protocols. These use a schedule that associates a time slot for each sensor node, helping to avoid collisions and reduce the effects of excessive listening and inactivity problems. These protocols require the presence of a management authority such as a dedicated access point to manage the schedule. Common MAC protocols in WSN include IEEE 802.11, S-MAC and T-MAC.

4.7.1. IEEE 802.11

This MAC protocol is based on CSMA/CA and implements control packets to avoid collision whenever possible. Power saving mode (PSM) reduces idle listening by periodically entering the sleep state. Unfortunately, this PSM is not suitable for multi-hop networks such as WSN and therefore cannot be used in WSN.

4.7.2. S-MAC

This MAC protocol is based on CSMA/CA and is a well-known WSN protocol. It is a modification of the IEEE 802.11 protocol.

Figure 4.2 shows the basic outline of this protocol. It is divided into two parts, a listening session and a sleeping session. The listening session enables sensor nodes to communicate with other nodes to exchange control packets. During the sleep session, nodes switch off their radios to save energy. The first part of the listening session is synchronization by sending SYNC packets. Each node maintains a schedule table that stores all the schedules (listening and sleeping sessions) of all its known neighbors. During synchronization, a node broadcasts its schedule to all its neighbors. After that, each node has a schedule of its neighbors and can use it to send data to its neighbors. Before a node wants to send data to its neighbor to organize a data exchange, it knows the neighbor's schedule, sends a packet (RTS - request to send) and waits for the neighbor's response. If the neighbor is ready to receive, it sends a CTS (clear to send) packet, and data transmission can begin immediately. Nodes not involved in any data transmission go into standby mode to save energy.

Using the synchronization packet (SYNC), each node now has its neighbor's schedule and can organize a data transfer, enabling this protocol to be used in a multi-hop network. It is necessary for each node to maintain its scheduling table after a certain number of scheduled synchronizations. Consequently, each node has to listen for a full period to find neighbors who may have different schedules. This causes packet overload and is the drawback of this protocol.

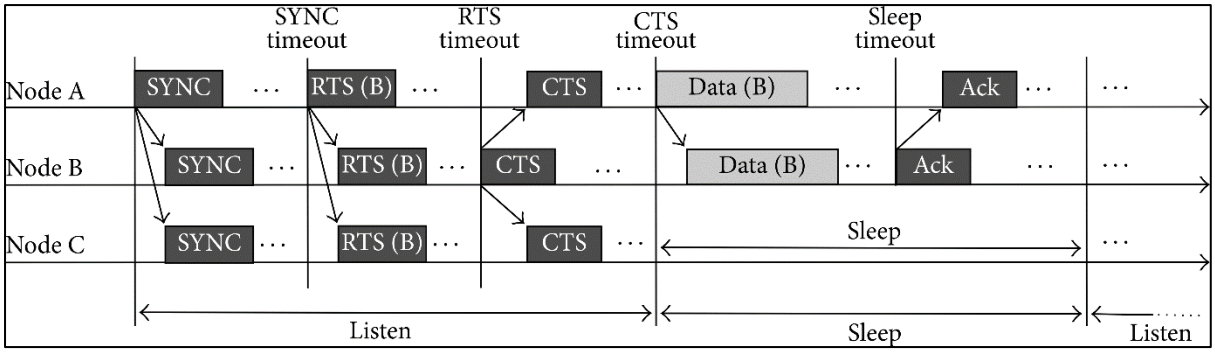


Figure 4.2. Basic schematic for S-MAC

4.7.3. T-MAC

T-MAC or Timeout MAC protocol is based on the S-MAC protocol and overcomes the S-MAC protocol by consuming less energy in terms of idle listening. Unlike S-MAC, this protocol keeps the listening session within a variable duration, which depends on network load. It defines a TA interval as the minimum amount of idle listening per frame. If a node wants to synchronize with its neighbor for a data transfer using SYNC and RTS/CTS, this TA interval is even greater than the exchange of these control packets. La Figure 4.3 shows that node A has organized a data transmission with node B. Node A has a different TC conflict interval than node C. If node B is ready for data transmission, it responds using a broadcast CTS packet. The TA interval must be long enough for node C to receive the start of the CTS packet. After this, node C automatically switches to standby mode to avoid idle listening.

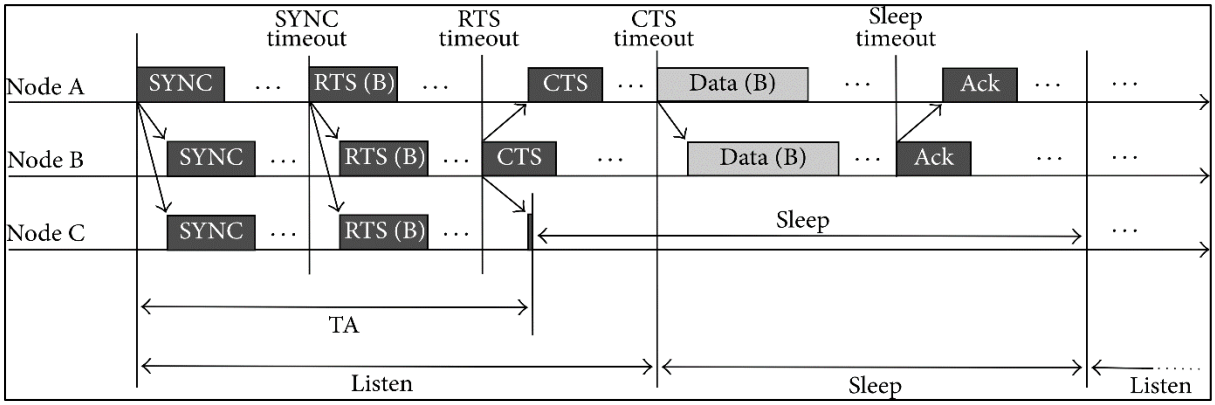


Figure 4.3. Basic schematic for T-MAC

4.8. Routing in sensor networks

Routing is the process of selecting the appropriate path for data to travel from source to destination. The process encounters several difficulties in route selection, which depends on network type, channel characteristics and performance metrics.

Data detected by sensor nodes in a wireless sensor network (WSN) is usually transmitted to the base station that connects the sensor network to other networks (perhaps the Internet), where the data is collected, analyzed and actioned accordingly.

In multi-hop communication, sensor nodes not only produce and deliver captured data, but also act as a path for other sensor nodes to the base station. The process of finding an appropriate path from the source node to the destination node is called routing, and is the primary responsibility of the network layer.

The basic classification of routing protocols is illustrated in the following figure:

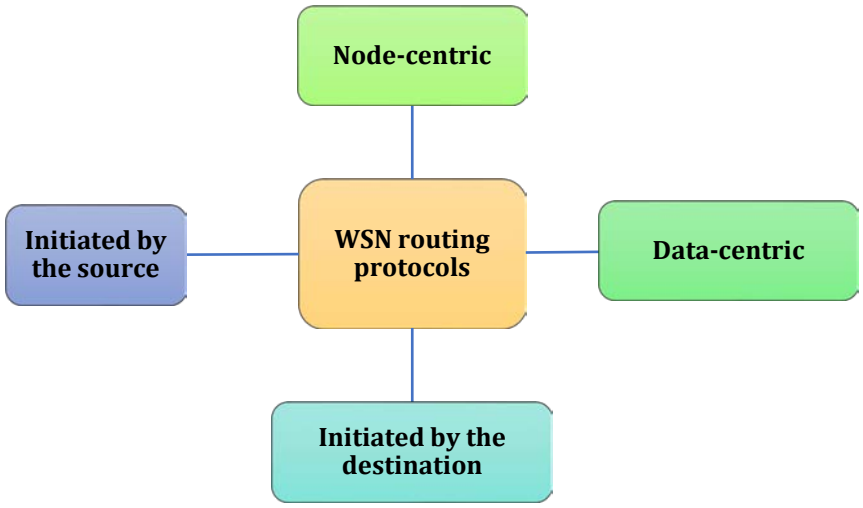


Figure 4.4. Classification of WSNs routing protocols

4.8.1. Node-centric

In node-centric protocols, the destination node is specified with certain numerical identifiers, and this type of communication is not expected in wireless sensor networks. For example, the LEACH protocol.

4.8.2. Data-centric

In most wireless sensor networks, the data or information detected is far more valuable than the node itself. Consequently, data-centric routing techniques focus primarily on transmitting information specified by certain attributes, rather than on collecting data from certain nodes. In data-centric routing, the receiving node queries specific regions to collect data of certain specific characteristics, so an attribute-based naming scheme is required to describe the characteristics of the data.

.

4.8.3. Destination-initiated protocols

Protocols are called destination-initiated protocols when the path configuration generation comes from the destination node. These include DD and LEACH.

4.8.4. Source-initiated

In these types of protocols, the source node announces when it has data to share, then the route is generated on the source side to the destination. The SPIN protocol is an example of this category.

4.9. Broadcast protocols for sensor networks

The simplest broadcast mode is flooding. The advantage of flooding is its simplicity and reliability. However, for its large number of redundant retransmissions, flooding will lead to severe packet collisions, wasted bandwidth and battery power depletion, which are called broadcast storm problems.

In flooding protocols, on receipt of a data packet by sensor nodes, this data packet is broadcast to all other neighbors. The broadcast process continues until one of two conditions is met: the packet has successfully reached its destination. And the second condition is that the maximum number of hops for a packet has been reached.

4.9.1. Low energy adaptive clustering hierarchy (LEACH)

LEACH is a routing protocol that organizes the cluster in such a way that energy is distributed equally across all the sensor nodes in the network. In the LEACH protocol, several clusters are generated from sensor nodes, with one node defined as the cluster leader and acting as the routing node for all other nodes in the cluster.

As in routing protocols, the cluster leader is selected before all communication begins, and communication fails if there is a problem in the cluster leader, and there is a high chance that the battery will die earlier than the other nodes in the cluster.

The LEACH protocol applies randomization and the cluster leader is selected from the group of nodes, so this selection of cluster leader from several nodes on a temporary basis makes this protocol more sustainable as the battery of a single node is not overcharged for long. The sensor nodes elect themselves as cluster leader with certain probability criteria defined by the protocol and announce this to the other nodes.

4.9.2. LEACH communication architecture

Similar to cellular networks, LEACH's communication architecture consists of forming cells based on signal amplitude, and using the cell heads as routers to the sink node. The cluster-heads (CH) are chosen randomly and periodically from among the nodes forming the cluster, depending on the state of its battery. They are then used as relays to reach the sink, following an algorithm that uses randomized rotation of cluster-heads to evenly distribute the energy load between network nodes. A sensor node decides which cluster to join based on the strength of the signals it receives. When the clusters are formed, as shown in Figure 4.5, all the ordinary nodes transmit their data to their CH, which aggregates it and transmits it, in turn, to the base station in unicast (single-hop) communication.

The CHs are tasked with performing the most energy-intensive functions, namely communication with the sink node, which is assumed to be remote, as well as all data processing (aggregation, fusion and transmission of data) in order to reduce the amount of data transmitted. This saves energy, since transmissions are only handled by the CHs, rather than by all the nodes in the network. As a result, LEACH achieves a significant reduction in energy dissipation.

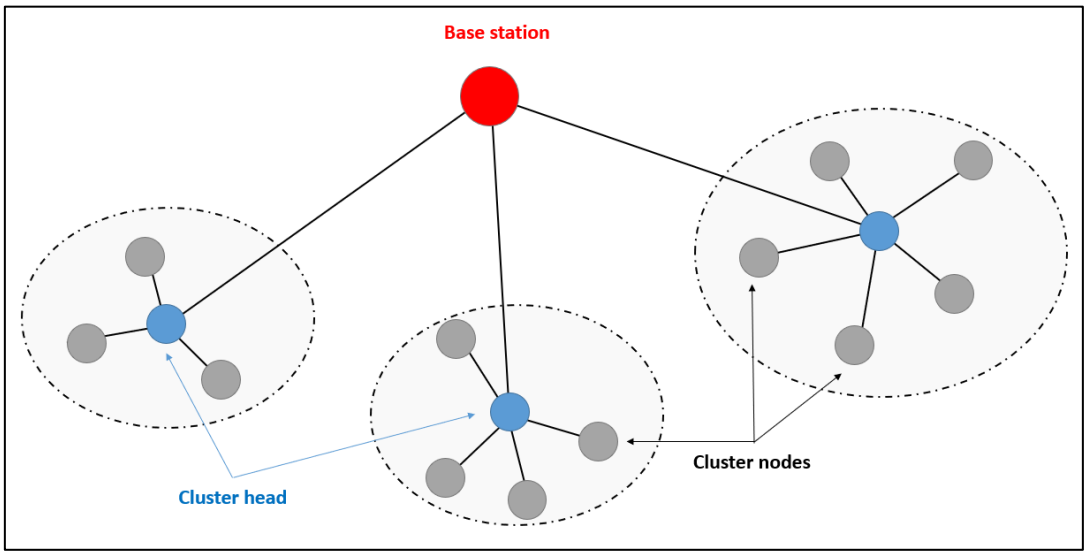


Figure 4.5. LEACH protocol communication architecture

4.9.3. How LEACH works

The LEACH protocol assumes equal residual sensor energies at the start of network operation. The life of the network is then segmented into rounds characterized by a choice of CH.

4.9.3.1. The set-up phases

Once each node has decided to which cluster it belongs, it must inform the cluster-head node that it will be a member of the cluster. Each node retransmits this information to the cluster-head again, using a CSMA MAC protocol. During this phase, all cluster-head nodes must keep their receivers switched on.

4.9.3.2. Scheduling

The cluster-head node receives all messages for nodes that would like to be included in the cluster. Based on the number of nodes in the cluster, the cluster-head node creates a TDMA schedule telling each node when it can transmit. This program is rebroadcast to the nodes in the cluster.

4.9.3.3. Data transmission

In this phase, data transfer to the base station takes place. Using the TDMA scheduler, members transmit their captured data during their own slots. This enables them to switch off their communication interfaces outside their slots to save energy. This data is then aggregated by the cluster-heads, merged and compressed, and sent to the base station. After a pre-determined period of time, the network moves on to a new round. This process is repeated until all the nodes in the network have been elected cluster-head once, throughout all the previous rounds. In this case, the round is reset to zero.

4.9.4. TEEN (Threshold sensitive Energy Efficient sensor Network protocol)

Most of TEEN's behavior is similar to the LEACH protocol. However, there are a few differences. Elected leaders do not transmit a TDMA schedule, but send a message containing the following information:

- Attributes: represent the task requested from the sensor.
- Hard threshold (HT): determines the critical value after which members must send their data report.
- Soft threshold (ST): specifies the minimum change requiring the node to send a new report.

So, when a node realizes that the captured value has exceeded HT, it must send a report to the boss. It only sends a new report if the value changes radically, i.e.: the difference exceeds ST. This mechanism makes it possible to implement reactive behavior, while limiting the number of messages used.

Given the reactive nature of TEEN, the use of TDMA is unsuitable. Several alternatives can be considered: CDMA or CSMA.

4.10. Energy management for sensor networks

Optimizing network lifetime is a major challenge. Maximizing the lifetime of a sensor network means minimizing the various ways in which energy is wasted. In fact, a sensor node consumes energy to accomplish its purpose in the network (data collection, processing and transmission).

4.10.1. Forms of energy dissipation

- **Sensing energy:**

The role of the sensing unit is to collect physical measurements of the monitored environment. It expands its energy in the following operations:

  - Data sampling and conversion into an electrical signal
  - Signal processing
  - converting the signal from analog to digital.

- **Processing energy (calculation):**

This unit consists of a microcontroller (microprocessor) and a memory. The residual energy of this unit is spent on switching and leakage. Switching energy is determined by the supply voltage and the total capacity switched at software level (by running software). Leakage energy, on the other hand, refers to the energy consumed by the computing unit when no processing is carried out.

- **Communication energy:**
  - The communication unit, whose role is to send and receive data, is the unit that consumes the most energy. Communication energy is determined by three factors:
  - The amount of data exchanged.
  - The distance between nodes.
  - The power of the radio: when the transmission power is high, the signal will have a long range and the energy consumed will be higher.

4.10.2. Factors involved in energy consumption

There are a number of factors that lead to unnecessary energy consumption (overconsumption):

4.10.2.1. Radio module status

The radio module is the most energy-intensive component of the sensor node, since it is responsible for communication between the nodes. The radio module operates in four modes: idle, transmit, receive and sleep.

- Idle state: the radio is switched on, but not in use. In other words, the sensor node is neither receiving nor transmitting.
- Transmit state: the radio is transmitting a packet.
- Receive state: the radio is receiving a packet.
- Sleep state: the radio is switched off.

4.10.2.2. Accessing the transmission medium

The MAC layer plays a key role in minimizing energy consumption. An energy-efficient MAC protocol tries to use the radio module as little as possible. Unnecessary use of the radio module comes from six main sources: retransmission, passive listening, eavesdropping, overloading, over transmission and packet size.

4.10.3. Energy conservation techniques

The three main energy-consuming tasks of a sensor node are: capture, processing and communication. Several approaches have been proposed to optimize energy for these three tasks. In addition, several classifications of these tasks have been proposed in the literature. We have chosen the classification shown in Figure 4.6, and we have also divided the prioritization methods into two classes.

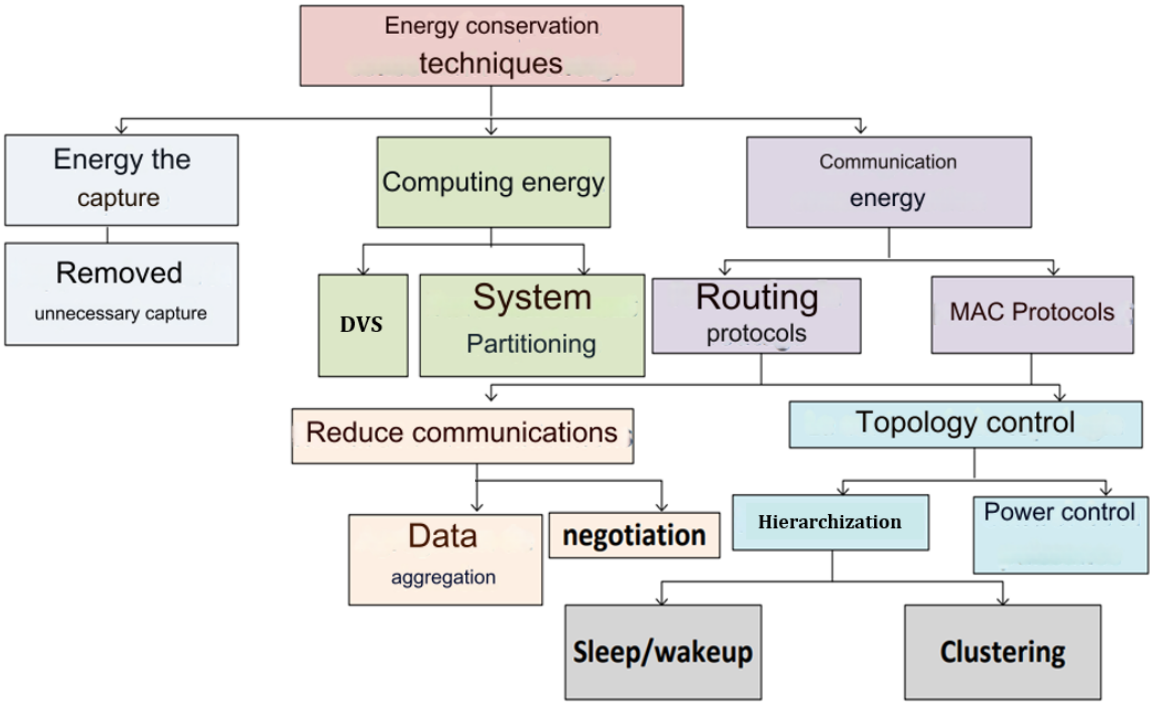


Figure 4.6. Energy conservation techniques

4.10.3.1. Techniques for dynamic adaptation of processor speed and voltage (DVS)

The energy expended by the computing unit is highly dependent on the supply voltage. As a result, minimizing computation energy expenditure is linked to minimizing voltage. This is why DVS has been proposed and deployed in microprocessors. DVS enables processors to change their voltage and adjust their frequency according to the application's requirements, without degrading performance. In this way, the DVS technique helps sensors to conserve their energy. The basic idea is to set the supply voltage so that the processor runs at a long rate when the processor workload is low. On the other hand, if the workload is high, then the DVS controls the processor to work at high speed.

4.10.3.2. Data aggregation

Since neighboring nodes in sensor networks are highly correlated spatially and temporally, they may generate the same data, which is then transferred to the base station (sink). At some point, intermediate nodes may have the same data received from source nodes. To eliminate this redundancy and minimize the amount of data transferred to the base station, data aggregation techniques are used.

4.10.3.3. Hierarchization

Hierarchical methods involve organizing the network into multi-level structures. There are two main families in this category: clustering methods and sleep/wakeup methods.

4.11. Overview of operating systems for sensor networks (TinyOS example)

The basic functionality of an operating system is to hide the low-level details of the sensor node by providing a clear interface to the outside world. Here are some of the low-level services that an operating system must provide:

- Processor management
- Memory management
- Device management
- Scheduling policies
- Multithreading
- Multitasking

In addition to the services mentioned above, the operating system must also provide services such as:

- Support for dynamic loading and unloading of modules
- Providing appropriate concurrency mechanisms
- Application Programming Interface (API) to access underlying hardware
- Enforce appropriate power management policies

TinyOS has been designed specifically for WSNs. It introduces a structured, event-driven execution model and a component-based software design that supports a high degree of concurrency in a small footprint, improves robustness and minimizes power consumption, while facilitating the implementation of sophisticated protocols and algorithms. The system and its services comprise connected components with well-defined interfaces, in much the same way as a wiring diagram connects hardware blocks. The diversity of hardware platforms, protocols and applications is addressed by connecting the necessary components from a catalog of candidates.

4.11.1. TinyOS features

Concurrence:

- Uses event-oriented architecture

Modularity:

- Application composed of components
- OS + Application compiled into a single executable

Communication:

- Uses an event/command model
- Non-preemptive FIFO scheduling
- No kernel/user separation

4.11.2. Overview of TinyOS

- Operating system for embedded sensor networks
- Set of software components that can be linked together into a single executable on a mote (sensor node)

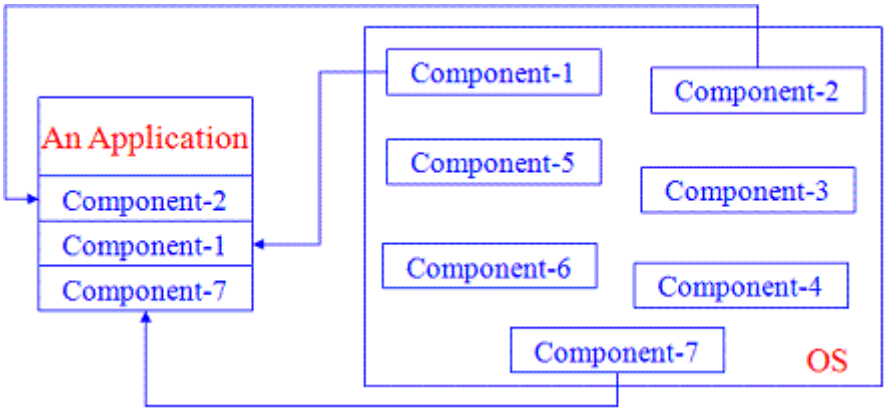


Figure 4.7. A set of software components

4.11.3. TinyOS memory model

Static memory allocation

- No heap (malloc)
- No pointer to function
- No dynamic allocation

Global variables

- Available per-frame
- Memory conservation
- Use of pointers

Local variables

- Saved on stack

- Declared in a method

4.12. Synchronization in sensor networks

Clock synchronization in a computer network aims to provide a common time scale for the local clocks of nodes in the network.

Time is needed to

- Date an event
- Evaluate the time between two events
- Order events

In distributed network synchronization we have no global clock or shared memory, but clock drifts. The definition of synchronization does not necessarily mean that all clocks are perfectly matched on the network. This would be the strictest form of synchronization, as well as the most difficult to implement. Precise clock synchronization is not always essential, so protocols ranging from the most lenient to the strictest are available to meet these needs. There are three basic types of synchronization method for wireless networks. The first is relative synchronization, and is the simplest. It is based on the order of messages and events. The basic idea is to be able to determine whether event 1 occurred before event 2, simply by comparing local clocks to determine the order. Clock synchronization is not important. The second method is relative synchronization, in which the clocks in the network are independent of each other, and the nodes keep track of the diversion and offset. Usually, a node keeps information on its drift and offset in correspondence with neighboring nodes. Nodes can synchronize their local time with the local time of another node at any time. Most synchronization protocols use this method.

The final method is global synchronization, where there is a constant global time scale throughout the network. This is obviously the most complex and difficult to implement. Very few synchronization algorithms use this method, mainly because this type of synchronization is generally unnecessary.

There are many different synchronization protocols, many of which are not very different from one another. As with any protocol, the basic idea is always there, but improving on the drawbacks is a constant evolution. Three protocols will be discussed in detail: Reference Broadcast Synchronization (RBS), Synchronization Protocol for Sensor Networks (TPSN) and Flood Time Synchronization Protocol (FTSP). These three protocols are the main synchronization protocols currently used for wireless networks.

There are other synchronization protocols, but these three represent a good illustration of the different types of protocols. All three-cover sender-receiver synchronization as well as receiver-receiver synchronization. They also cover single-hop and multi-hop synchronization schemes.

4.12.1. Reference Broadcast Synchronization

Many time synchronization protocols use a sender-receiver synchronization method in which the sender transmits timestamp information and the receiver synchronizes. RBS is different in that it uses "receiver-to-receiver" synchronization. The idea is that a third party will broadcast a beacon to all receivers. The beacon contains no time information; instead, the receivers will compare their clocks with each other to calculate their relative phase shifts. Synchronization is based on when the node receives the reference beacon.

The simplest form of RBS is one broadcast beacon and two receivers. The synchronization packet is broadcast to both receivers. The receivers will record when the packet was received according to their local clocks. Then, the two receivers exchange their time information and can calculate the offset. This information is sufficient to retain a local time scale.

RBS can be extended from the simplest form of one broadcast and two receivers to synchronization between n receivers. This may require sending more than one broadcast. Increasing the number of broadcasts will increase the precision of the synchronization.

RBS differs from traditional sender-receiver synchronization by using receiver-receiver synchronization. The reference beacon is broadcast to all nodes. Once received, the receivers note their local time and then exchange time information with their neighboring nodes. The nodes can then calculate their offset.

4.13. Security in sensor networks

Security, confidentiality, computational and energy constraints, and reliability issues are the main challenges facing WSNs, particularly during routing. To solve these problems, WSN routing protocols need to guarantee confidentiality, integrity, privacy preservation and network reliability. Efficient, energy-saving countermeasures must be designed to prevent intrusion into the network.

4.13.1. Attacks and solutions in WSNs

The most well-known attacks on WSNs are described below.

4.13.1.1. Manipulation of routing information

This attack targets routing information between two sensor nodes. It can be launched by falsifying or replaying routing information. This can be done by adversaries who have the ability to create routing loops, attract or repel network traffic and extend or shorten source routes. This is a passive attack that is not only easy to launch, but elusive to detection. However, a unique identity can be created for the selected path, using the hash function based on the key of the pseudonyms or identities of all the selected intermediate nodes and embellished in the message. Any attempt to register a data packet from one location and re-tunnel it to another location will be detected by the base station when comparing the embellished path identity with the hash of all the added pseudonyms or identities of all the nodes involved in the multi-hop.

4.13.1.2. Sybil attack

In this attack, the adversary compromises the WSN by creating false identities to disrupt network protocols. The Sybil attack can lead to a denial of service. It can also affect mapping during routing, as a Sybil node creates illegal identities with the aim of breaking the one-to-one mapping between each node. Sybil is common in P2P networks, and also extends to wireless sensor networks. Moreover, detecting and defending against Sybil attacks is more difficult; this is due to the limited energy and computational capabilities of WSNs. Various efforts had been developed to counter the Sybil attack in WSNs. One example is the use of a pairwise key-based detection scheme that sets a threshold for the identity number a node can use. However, this requires pre-allocation of keys to the sensor node. Another way of thwarting the Sybil attack is to validate the identity of each node involved in routing.

4.13.1.3. Sinkhole attack

This attack prevents the receiving node (base station) from obtaining complete and correct sensor data, posing a threat to higher-layer applications. In this attack, an adversary makes itself attractive to its neighboring nodes in order to direct more traffic towards it. As a result, the adversary attracts all traffic destined for the receiving node. The adversary can then launch a more severe attack on the network, such as selectively forwarding, modifying or dropping packets. WSN is more vulnerable to this attack, as its nodes mostly send data to the base station.

4.13.1.4. Cloning attack

In a clone attack, the attacker first attacks and captures legitimate WSN sensor nodes, collects all their information from their memories, copies it onto several sensor nodes to create clone nodes, and finally deploys them on the network. Once a node has been cloned, the adversary can then launch further attacks. There are two different ways of detecting this attack: centralized and distributed approaches. Centralization uses the receiving node to detect and thwart the activities of clone nodes, while the distributed approach uses selected nodes to detect clone nodes and thwart their activities in the network.

Complement:

WSN constraints mainly determine the type of security approaches that can be adopted.

Chapter 05 : Vehicular networks

5.1. Introduction

VANET (Vehicular Ad Hoc Networks) is a subclass of mobile ad hoc networks (MANET), where it is developed by moving vehicles. VANET is a special case of a multi-hop wireless network, which has the constraint of rapid topology changes due to the high mobility of the nodes. With the growing number of vehicles equipped with computing technologies and wireless communication devices, inter-vehicle communication is becoming a promising area for research, standardization and development. In this chapter, we will outline the application areas of VANETs and look at the MAC layer and routing in vehicular networks.

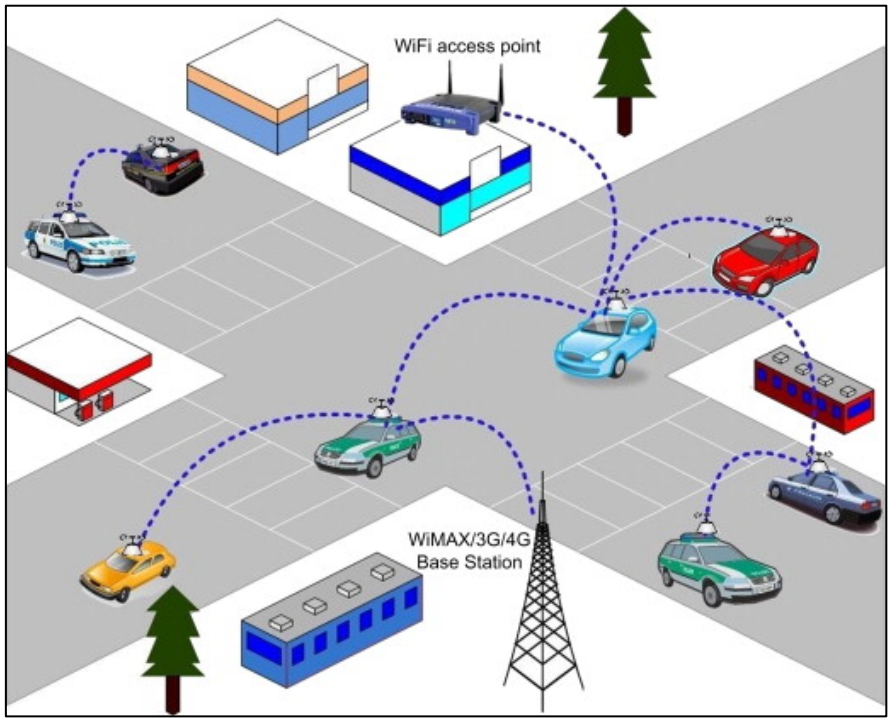


Figure 5.1. Example of a vehicular network

5.2. Main applications

Vehicle applications are generally classified into:

- **Active road safety applications:**

These aim to avoid the risk of car accidents and make driving safer by broadcasting information about hazards and obstacles. The basic idea is to broaden the driver's field

of perception, enabling him or her to react much more quickly, thanks to the reception of alerts via wireless communications. VANETs' main objective is to enable safety applications, while non-safety applications are expected to create business opportunities by increasing the number of vehicles equipped with on-board wireless devices.

- **Traffic efficiency and management applications:**

This category aims to optimize vehicle flows by reducing journey times and avoiding traffic jams. Applications such as enhanced route guidance/navigation, optimal traffic light programming and lane merging assistance aim to optimize routes, while reducing gas emissions and fuel consumption.

- **Comfort and infotainment applications:**

Comfort and infotainment applications aim to provide the road traveler with information and entertainment support to make the journey more enjoyable.

5.3. Study of the Mac and physical layer

The specific characteristics of VANETs make their quantitative and qualitative analysis particularly critical, especially when designing media access control (MAC) layer protocols. Although VANETs are considered a class of mobile ad hoc networks (MANETs), they have a number of specific characteristics that make many solutions for general MANETs unsuitable for VANETs. Some of the VANET characteristics that influence the design of an ideal MAC protocol are:

- **Number of nodes:** The density of nodes in a VANET can vary. It can be small, as in rural areas, or large, as at peak times in a big city. It's important to have a MAC protocol that can handle both cases. The main challenge in rural areas is network disconnection, while scalability is the main challenge in high-density areas.
- **High node mobility:** VANET nodes can move at very high speeds (160 km/h), which can lead to frequent disconnections between nodes. If a node is moving at very high speed (140 km/h) and is connected to a node that is moving at very low speed (30 km/h), the lifetime of the link will be short.
- **Predictable network topology:** The movement of nodes in a VANET is somewhat predictable, as the movement of nodes is limited by the topology of the route.

- **Frequent changes in network topology:** Due to the high mobility of nodes, the network topology in a VANET changes very frequently. It is important to have a MAC protocol capable of adapting to frequent topology changes in a transparent way.
- **Availability of location information:** Location information can be provided by having a GPS (Global Positioning System) receiver on board. Having such information available for communications can not only reduce message broadcast delivery latency, but can also increase system throughput.
- **Infrastructure support:** Unlike most MANETs, VANETs can take advantage of roadside infrastructure. This could improve the performance of VANET MAC protocols.
- **No power limit:** Unlike MANET nodes, VANET nodes have no power limit. They depend on a good power supply (e.g., the vehicle battery). This gives the nodes better computing resources.

5.3.1. IEEE standards for mac protocols (VANET)

In the USA, the Federal Communications Commission has allocated 75MHz of spectrum at 5.9 GHz for Dedicated Short-Range Communications (DSRC), which provides high-speed communication between vehicles and roadside units. DSRC is divided into seven channels, each 10 MHz wide, as shown in Figure 5.2 Channel 178 is the control channel (CCH), which is used for beacon messages, event-driven emergency messages and service announcements. The remaining six service channels (SCHs) support non-safety-related applications provided by roadside units.

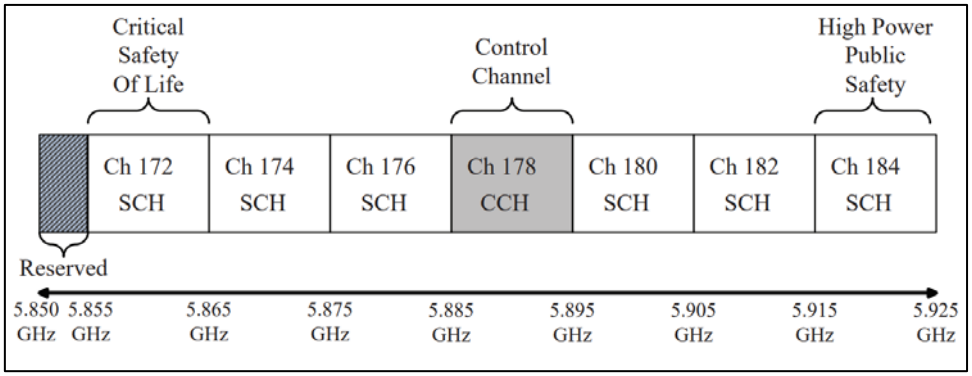


Figure 5.2. DSRC spectrum allocation in the USA.

The IEEE has completed the 1609 family of standards with the WAVE (Wireless Access in Vehicular Environments) standard for vehicular communications. In the remainder of this section, we explain the WAVE standard.

5.3.1.1. IEEE 1609 WAVE standards

IEEE 1609 WAVE is a family of standards for vehicle-to-vehicle and vehicle-to-infrastructure communication. WAVE specifies the following standards, as illustrated in Figure 5.3 :

- IEEE 1609.1 specifies the services and interfaces of the WAVE resource manager
- IEEE 1609.2 defines the formats and processing of secure messages
- IEEE 1609.3 presents transport and network layer protocols, including addressing and routing, in support of secure WAVE data exchange
- IEEE 1609.4 specifies the MAC and PHY layers, which are based on IEEE 802.11

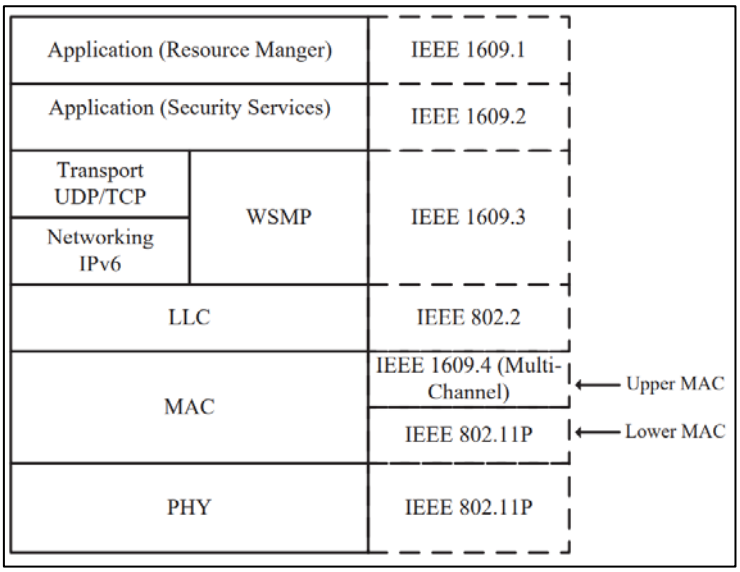


Figure 5.3. The WAVE protocol stack.

5.3.1.2. The IEEE 1609.4 standard

In WAVE, the IEEE 1609.4 standard operates above IEEE 802.11p in the MAC layer. IEEE 1609.4 focuses primarily on handling multi-channel DSRC radio operations, as illustrated in the figure below.

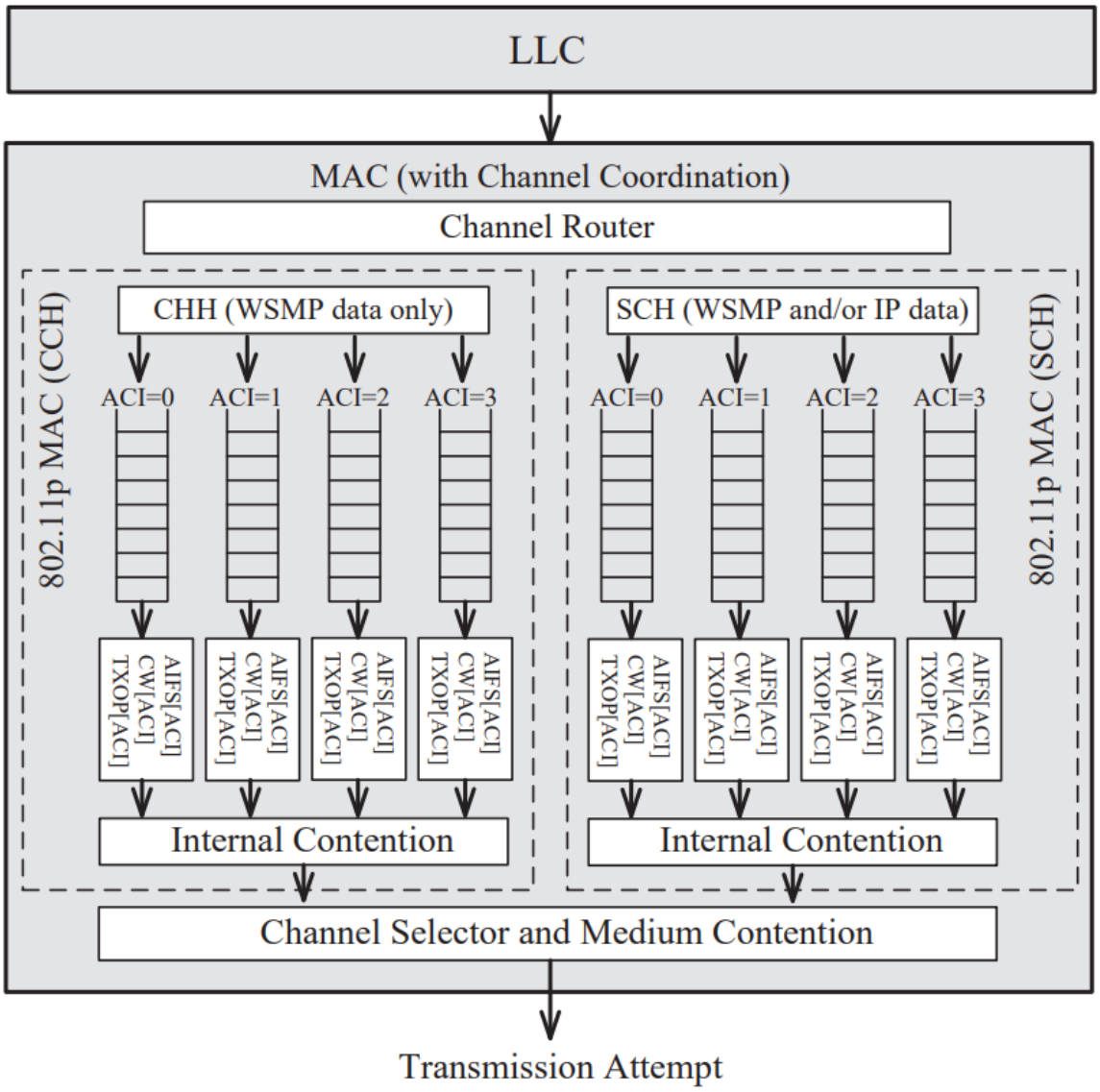


Figure 5.4. Reference architecture for MAC channel coordination

There is a synchronization interval (SI) consisting of a CCH interval (CCHI) and a SCH interval (SCHI), each separated by a guard interval, as illustrated in the figure above. All radio devices are supposed to be synchronized using a global positioning system (GPS). During CCHI, all radios should be tuned to CCH to broadcast updates and listen for messages from neighbors and roadside units. During SCHI, vehicles can tune in to the SCH of their choice, depending on the services on offer.

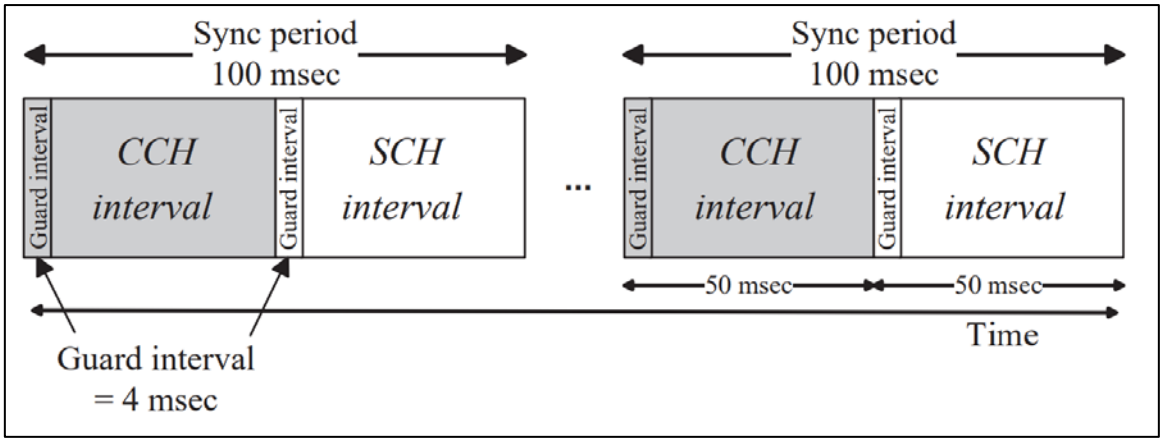


Figure 5.5. Time division into CCH intervals and SCH intervals, IEEE 1609.4 standard

The standard defines the length of the SI at 100 MS, based on the desire to have 10 security messages sent per second. It also defines a guard interval (GI) at the start of each CCHI and SCHI. The purpose of the GI is to take account of channel switching. Currently, the GI value is 4 to 6 MS, which corresponds to the time required for a radio to be tuned and made available on another channel.

5.3.1.3. The IEEE 802.11p standard

The IEEE 802.11p standard is the basis for the IEEE 1609 WAVE family of standards. It defines the physical and media access control layers. The WAVE stack uses IEEE-802.11p, which is based on CSMA/CA as defined in IEEE 802.11 as the MAC protocol; it includes the QoS amendments of IEEE-802.11e. Recently, the IEEE completed work on the 802.11p LAN standard, which uses IEEE 802.11e Enhanced Distributed Channel Access (EDCA). Figure 5.4 gives an overview of the EDCA architecture and the type of channels supported, CCH and SCH.

For IEEE 802.11p, different inter-frame arbitration spaces (AIFS) and contention window (CW) values are chosen for different application categories (AC). There are four categories of data traffic available with different priorities: background traffic (BK - Bulk), best effort traffic (BE - Bulk Effort), voice traffic (VO - Voice) and video traffic (VI - Video). Each category of data traffic has its own queue; there are four different queues for each channel. Table 5.1 shows parameter settings for different application categories in IEEE 802.11p.

Due to the nature of VANET, IEEE 802.11p must have different MAC operations than IEEE 802.11. Here is a brief description of some of the changes to IEEE 802.11 MAC:

- **WAVE mode:** Since security communications in VANETs require fast data exchange, IEEE 802.11 MAC operations take too long. Scanning channels for a Basic Service Set (BSS) tag and performing multiple handshakes to establish communications is not affordable. Therefore, in WAVE mode, vehicles are on the same channel and the same BSSID to communicate at no extra cost.
- **WAVE BSS:** The WAVE standard defines a new type of BSS, WAVE BSS (WBSS). When a "vehicle/roadside unit" wishes to form a WBSS, it transmits a beacon on request. This beacon has a specific format and is used to announce a WAVE BSS.

Table 5.1. IEEE 802.11p parameter settings for different application categories

AC	CW_{min}	CW_{max}	AIFSN
VI	3	7	2
VO	3	7	3
BE	7	225	6
BK	15	1023	9

5.4. Routing in vehicular networks

VANET routing protocols must be designed taking into account factors such as security, mobility and scalability of vehicular communication.

The aim of VANET architecture is to enable connection between vehicles, or between vehicles and roadside units, leading to the following three possibilities:

Ad hoc vehicle-to-vehicle (V2V) network: enables direct vehicular communication without dependence on a fixed infrastructure medium, and can be used primarily for security, safety and broadcast applications.

Vehicle-to-infrastructure (V2I) network: enables a vehicle to communicate with the roadside unit, mainly for information and data collection applications.

Hybrid architecture: combines both V2I and V2V communications. In this scenario, a vehicle can communicate with the roadside infrastructure on a multi-hop or single-hop basis, depending on distance, i.e., whether or not it can access the roadside unit directly. It enables long-distance connection to the Internet or to remote vehicles.

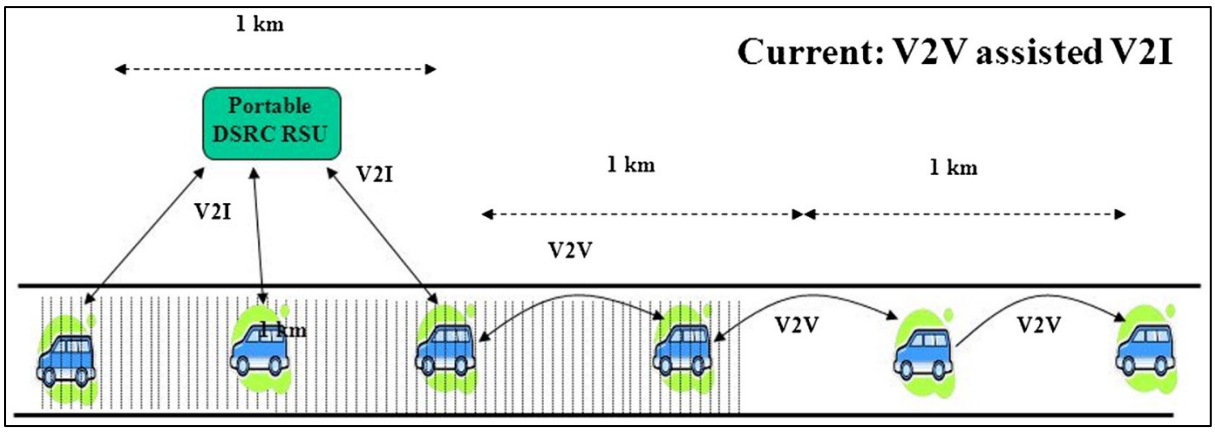


Figure 5.6. V2I and V2V structure

The high dynamic topology characteristics make the efficient design of VANET routing protocols more difficult. VANET routing protocols can be classified into two categories, such as topology-based routing protocols and position-based routing protocols.

The following figure describes a set of VANET routing protocols according to their methodology and mechanism.

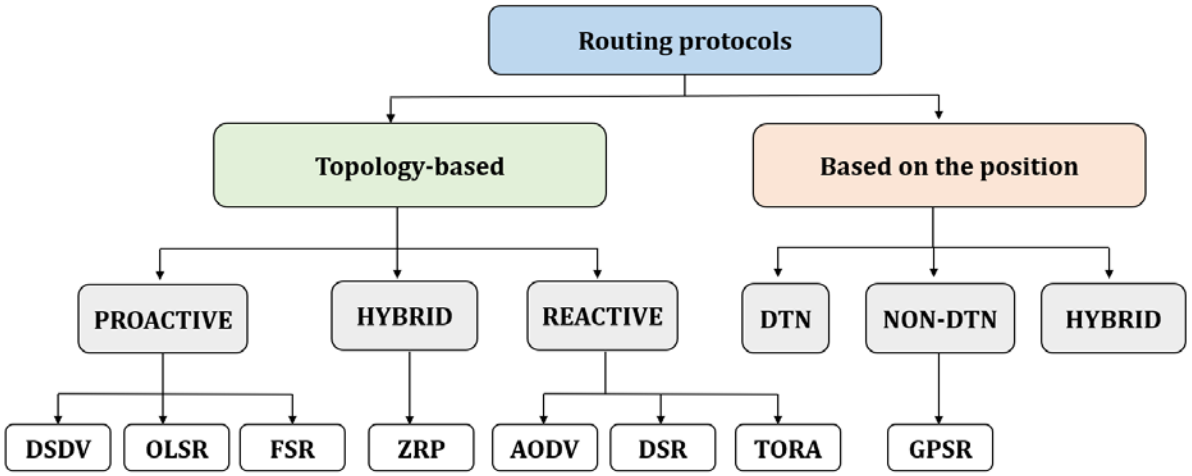


Figure 5.7. VANET routing protocols

5.4.1. Topology-based routing protocols

These use link information to transmit data packets between nodes via the VANET. There are two sub-categories within this mechanism, the proactive approach, which depends on routing techniques related to the table-based methodology, and the reactive approach, which depends on routing techniques related to the on-demand methodology.

- **Proactive routing protocols:**

Generally, depend on algorithms linked to the shortest route. They store all data relating to connected nodes in predefined tables, which are the main mechanism of these routing

protocols. This data is also shared with partner nodes. Each routing table is updated by its node when the network topology is modified by an event.

Advantages:

- Low-latency, real-time applications.
- No need for path discovery.

Limitations:

- A large proportion of available bandwidth is taken up by unused routes.

- **Reactive routing protocols:**

Reactive routing protocols generally depend on algorithms linked to on-demand actions. When two nodes want to communicate, they initiate path discovery, and one of its main advantages is the reduction in network traffic.

- **Advantages:**
  - Flooding is required when requested, so there's no need for proactive overflow in the network.
  - It controls bandwidth because it is Beaconless.
- **Limitations:**
  - Disruption to node communication occurred due to exaggerated network flooding.
  - High path search latency

5.4.2. Position-based routing protocols

Depend on algorithms linked to the positioning mechanism using location-based applications (e.g., GPS). Such applications provide such data for path selection. Furthermore, these protocols do not process any tables linked to routing data, nor any information linked to the state of the join with neighboring nodes.

5.4.3. OLSR

OSLR (optimized link state routing) stands for optimized link state routing, i.e. a routing protocol using proactive mode. Whenever a topology change occurs, the MPRs (multipoint relays) are responsible for generating and transmitting topology information to the selected nodes.

This is a proactive protocol based on table-driven methodology. According to its name, the link-state scheme is used by this protocol in an enhanced way to circulate topology

information. OLSR also uses this mechanism, but in order to maintain bandwidth, message overflow in OLSR is enhanced as the protocol operates in wireless multi-hop scenarios.

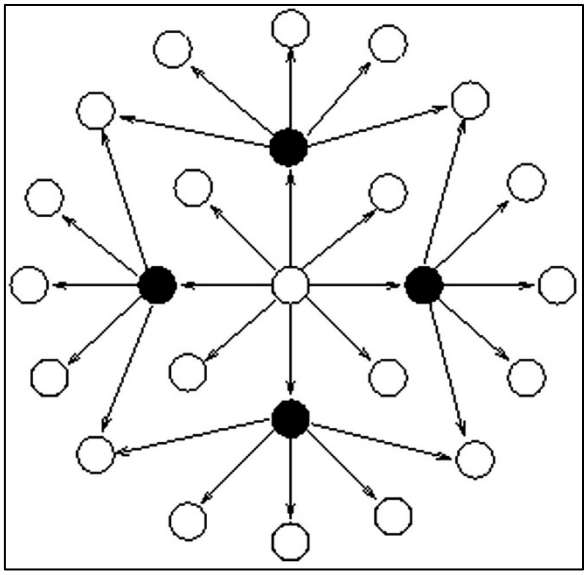


Figure 5.8. Flooding a packet in a multi-hop wireless network from the central node using MPR

As a table-based OLSR protocol, OLSR basically manages and updates information in a set of tables. These tables include data based on the control traffic received, and control traffic is generated on the basis of the information returned by these tables. The tables also manage the route calculation itself. OLSR uses the following essential control message types:

- Topology control messages (TC).
- HELLO control messages (HELLO).
- Multiple interface declaration messages (MID).

Advantages:

In the broadcast scenario, reduce the number of packet retransmissions.

Limitation:

In OLSR, a large amount of bandwidth and CPU power is required to calculate the optimal path.

5.4.4. GPSR

GPSR (Greedy perimeter stateless routing) is a position-based routing protocol. GPSR archives evolved in terms of the number of nodes in the network and the rate of mobility,

storing little information per node. It stores only the node identifier and the node's physical location in a routing table. GPSR operates in two modes:

- In greedy mode, packets are forwarded to a node geographically closer to a destination node.
- If greedy fails, it switches to perimeter transfer mode. In this mode, packets are forwarded along the node's perimeter. When it finds a node closer to the destination, it switches back to greedy mode. This protocol performs well at high mobility rates. However, GPSR has a disadvantage in that a large number of packets are lost due to the formation of routing loops in perimeter transfer mode.

5.5. Mobility model and simulation

Several mobility models and tools are available for traffic model generation. The mobility model is designed to describe the movement pattern of mobile users, and how their location, speed and acceleration change over time. Mobility models are generally classified into macroscopic mobility models and microscopic mobility models.

5.5.1. Macroscopic mobility model

This type of mobility model takes account of movement constraints such as streets, roads, junctions and traffic lights when generating vehicle movement traces. They define vehicle traffic generation such as traffic flow, traffic density and initial vehicle distribution.

5.5.1.1. Random mobility model

In the random way point model, mobile nodes move randomly and freely without any restrictions. In this model, destination, speed and direction are all chosen at random and independently of other nodes. The fraction of nodes in the network remains static throughout the simulation. Node speed is uniformly chosen at random in the interval [Vmin, Vmax]. The node moves towards the destination with speed V. When it reaches the destination, it remains static for the predefined pause time and then moves again according to the same rule. Node mobility behavior is highly dependent on pause time and maximum node speed. The following parameters describe a model simulation configuration.

- Size and shape of the deployment zone
- Initial spatial distribution of nodes
- Probability density function of pause time

- Minimum and maximum speed

5.5.1.2. Gauss Markov model

The Gauss Markov model first calculates the velocity and direction of movement for each node. Then, the nodes move with the calculated speed and direction for a period. After this period, similar movements begin again. The time used in the movement in each interval before the change of speed and direction is constant.

5.5.1.3. Manhattan mobility model

This model describes the VANET simulation of traffic mobility in the city of Manhattan. In this model, the movement of each node is confined by the direction of the road. Within a road, there are two directions. This model consists of horizontal and vertical lines for its route. In this model, there are four directions, i.e., north and south for the vertical direction, and east and west for the horizontal directions. For intersections that consist of a vertical and horizontal direction, the node can move straight ahead or stay on its route, or it can turn right or left. The probability of going straight is 0.5, the probability of turning right is 0.25 and the probability of turning left is 0.25.

The speed of the node in the current time interval depends on the previous time intervals. Moreover, a node's speed is confined by the speed of another node to precede it on the same route. Mobility in the Manhattan model is highly dependent on space and time boundaries. This model forces the node to follow geographical constraints such as roadblocks, etc.

5.5.2. Microscopic mobility model

5.5.2.1. Street Random Way point (STRAW)

Is a tool that generates mobility patterns by extracting urban topologies from the TIGER database. It supports the micro-mobility functionalities of the models. STRAW implements complex intersection management using traffic lights and signs. This feature gives the vehicle a more realistic behavior when reaching an intersection. It includes traffic control mechanisms that force drivers to follow a deterministic admission control protocol when encountering an intersection. The disadvantage of the STRAW model is that it does not give details of traffic flows. In addition, it does not specify lane-changing behavior.

5.5.2.2. CanuMobiSim

Is a tool for generating motion traces under various conditions. This tool provides a graphical interface for generating mobility models, and can generate mobility traces for the Network Simulator and GloMoSim.

The CanuMobiSim tool takes micro-mobility into account and implements several car-to-car interaction models that adjust vehicle speed according to vehicle density. It also implements an intelligent driver model, which adapts speed according to movements between neighboring vehicles. The CanuMobiSim tool includes complex traffic generators that can implement basic source-destination paths using Dijkstra algorithms. But due to its generic structure, it suffers from a problem of reduced level of detail in specific scenarios.

5.5.2.3. VanetMobiSim

Is a tool that generates realistic vehicle motion traces. It is an extension of CanuMobiSim. As CanuMobiSim provides an efficient and easily extensible mobility architecture, but due to its general-purpose nature, it suffers from a reduced level of detail in specific scenarios. VanetMobiSim aims to extend CanuMobiSim's vehicular mobility support to a higher degree of realism. In VanetMobiSim, the micro-mobility functionality takes into account road topology, road structure (unidirectional or bidirectional, single-lane or multi-lane), road characteristics (speed limits, vehicle class restrictions) and the presence of traffic signs.

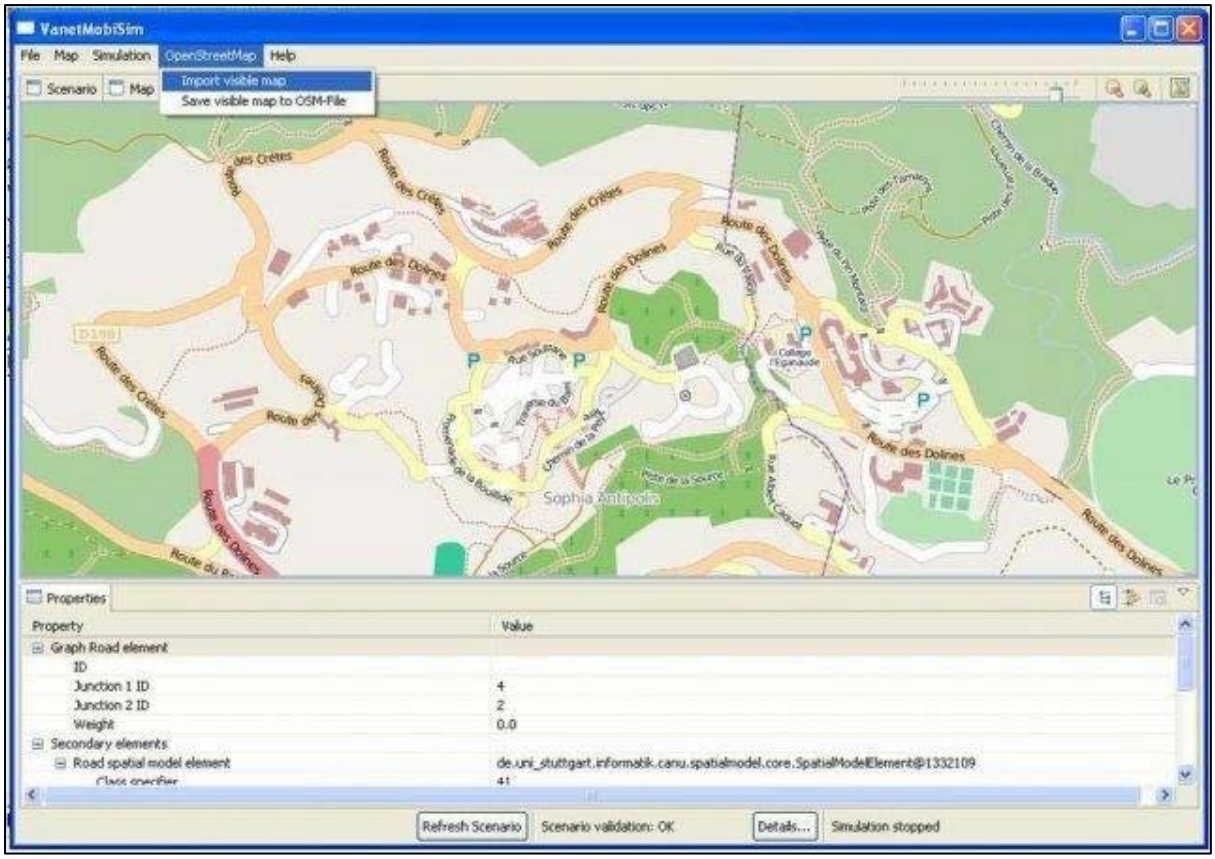


Figure 5.9. VanetMobiSim

5.6. VANET security

Security in VANETs is of particular concern because human lives are constantly at stake, whereas in traditional networks, the main security issues include confidentiality, integrity and availability, none of which primarily involve personal safety. Vital information cannot be altered or deleted by an attacker. Nevertheless, security in VANET also indicates the ability to determine driver responsibility while preserving driver confidentiality. Information about the vehicles and their drivers inside must be exchanged securely and, more importantly, in a timely manner, as delays in message exchange can lead to catastrophic consequences such as a vehicle collision.

5.6.1. Attack classification and proposed solutions

VANETs are exposed to a variety of threats and attacks. Since the vehicle itself is a sufficient source of electricity, the onboard unit doesn't have to endure the bottleneck of limited battery life like other mobile devices such as smartphones and wearables. As a result, we can integrate all kinds of processors and chips into the onboard unit to give the vehicle workstation-scale computing capacity. Unfortunately, this advantage is only one

side of the coin. Such computing capacity also enables attacks that are computationally intensive and not feasible in normal ad hoc networks.

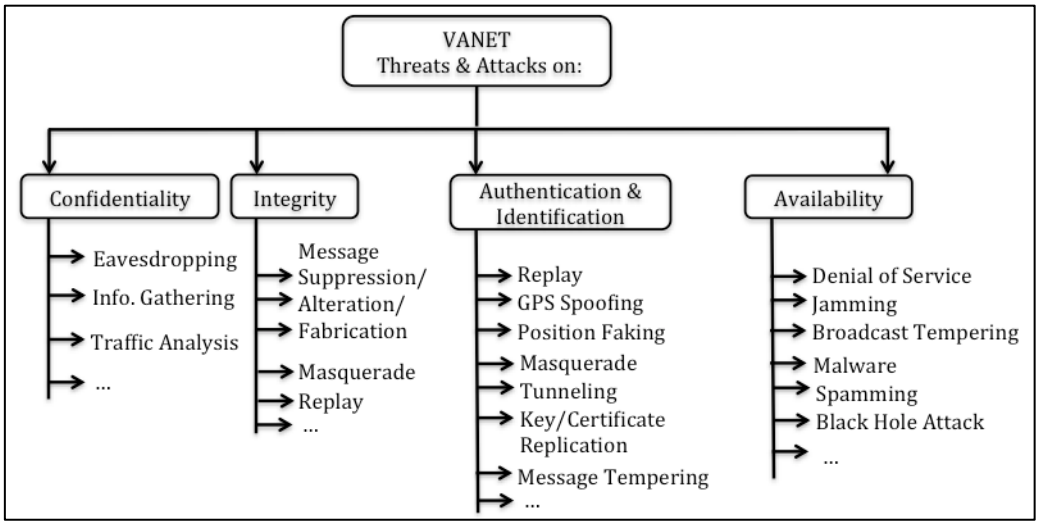


Figure 5.10. Classification and examples of VANET attacks

Table 5.2. Major attacks, cryptographic solutions and proposals.

Attacks	**Targeted service**	**Cryptographic solutions and proposals**
Jamming	Availability	Pseudorandom Frequency Hopping
Eavesdropping	Confidentiality	Encryption on Sensitive Messages
Traffic analysis	Confidentiality	Randomizing Traffic Patterns
DOS	Availability	Signature-based Authentication and Access Control
Editing messages	Integrity	Integrity Metrics for Content Delivery
Brute Force	Confidentiality	Public Key Schemes
Illusion/Identity fraud	Authentication	Trusted Hardware Module
Position simulation	Authentication	Active Detection Systems
Illegal tracking	Privacy	ID-based System for User Privacy

Chapter 06 : Network security

6.1. Introduction

Network security is the protection of the network infrastructure against unauthorized access, misuse or theft. It involves creating a secure infrastructure so that devices, applications and users can operate securely. Network security combines several layers of defense at the edge and within the network, with each network security layer implementing policies and controls. Authorized users access network resources, but malicious actors are prevented from carrying out exploits and threats.

6.2. Single sign-on (SSO)

Single sign-on (SSO) is an authentication method that enables users to securely authenticate themselves to multiple applications and websites using a single set of credentials. As users frequently access applications directly from their browsers, companies are turning to access management strategies that improve both security and user experience. Single sign-on offers both, as users can access all password-protected resources without having to log in again once their identity has been validated.

It enables a user to use a single set of credentials to access multiple applications. Single sign-on can be used by enterprises, small and medium-sized businesses and individuals to facilitate the management of multiple credentials. OAuth and SAML are two protocols used to authorize access, SAML works by exchanging user information such as logins, authentication status, credentials and other relevant attributes between the identity provider and the service provider.

6.2.1. How it works?

Single sign-on works on the basis of a trust relationship established between an application, known as a service provider, and an identity provider. This trust relationship is often based on a certificate exchanged between the identity provider and the service provider. This certificate can be used to sign identity information sent by the identity provider to the service provider, so that the service provider knows it has come from a trusted source.

In SSO (Identity Provider), this identity data takes the form of tokens containing identifying information about the user, such as a user's e-mail address or username.

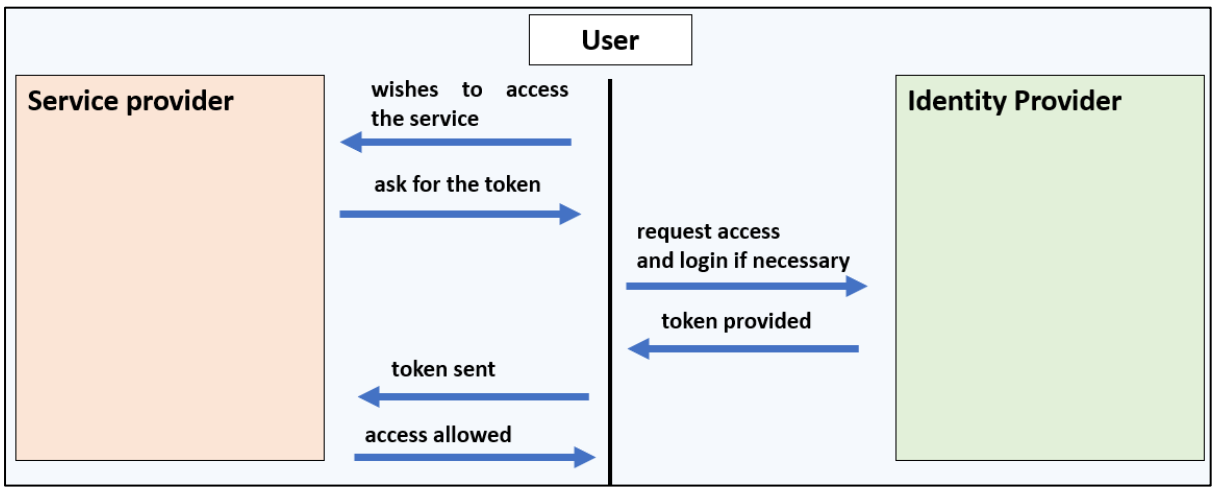


Figure 6.1. SSO operations

6.2.2. The SSO token

An SSO token is a collection of data or information transmitted from one system to another during the SSO process. The data may simply be a user's e-mail address and information about the system sending the token.

Tokens need to be digitally signed so that the token recipient can verify that the token has come from a trusted source. The certificate used for this digital signature is exchanged during the initial configuration process.

6.3. DNS Securing DNS

DNS (Domain Name System) is a directory service that provides a mapping between the name of a host on the network and its numerical address. DNS is essential to the operation of the Internet. Each node in a tree has a domain name, and a complete domain name made up of a sequence of symbols specified by dots. DNS is a service that translates domain names into IP addresses, enabling network users to use easy names when searching for other hosts, rather than remembering IP addresses.

6.3.1. Major attacks

6.3.1.1. DDoS attacks

There are many different types of Distributed Denial of Service (DDoS) attack.

This type of attack is used to overwhelm DNS servers, making DNS service unavailable. When a DNS attack succeeds, it can cruelly immobilize an organization. When a company can't publish the addresses of its web and mail servers, business grinds to a halt.

6.3.1.1.1. Amplification

An amplification attack is a technique in which a small request can trigger a large response, such as the request for a TXT record. By flooding the server with short queries that require long responses, even a relatively weak computer can overload a DNS server. The DNS server is so busy doing the hard work of answering all these fake queries that it doesn't have time to answer the legitimate ones.

If a user makes a DNS query for "re.dz", the query size is 50 bytes and the response is 4092 bytes (about 80 times amplification). Let's assume that an attacker is generating queries with a botnet (a network of independent hosts, or bots, infected with malware), and that each bot has a 2 Mbps connection to the Internet. With a 2 Mbps connection, each bot can send the 50-byte request in the previous example around 5242 times per second. If the botnet contains 100 bots all doing the same thing, that's a total of 2 gigabytes that the DNS server is expected to send every second of the attack. Amplification alone is an effective attack, as attackers can use less powerful resources to overload powerful servers.

6.3.1.1.2. Reflection

A reflection attack sends requests that appear to come from the attack victim. The response (often a large, amplified response) is sent to the victim, who never asked. The amount of response traffic could potentially overwhelm the victim's network.

In a reflection attack, an attacker sends a query to a recursive name server with a spoofed source IP address. Instead of his real IP address, he sets the target (victim) IP address as the source IP address. The recursive name server does the work, retrieves the response to the query from the authoritative name server and sends the response to the unsuspecting victim.

6.3.1.1.3. Hybrid attack (Amplification + Reflection)

The attacker spoofs the victim's IP address and sends a precisely crafted request, resulting in a high payload. This is a highly effective DDoS attack, with the authoritative name server providing the amplification and the recursive name server providing the

reflection. This allows the attacker to attack two different victims at the same time. It also provokes the victim of the amplification attack to eventually believe that he has been attacked by the second victim, potentially causing even more chaos.

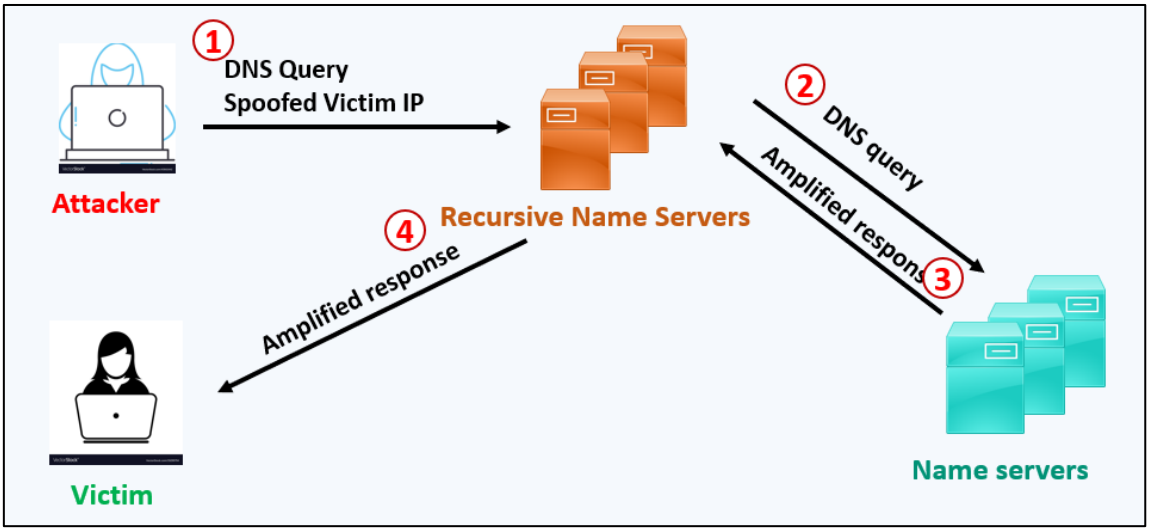


Figure 6.2. A hybrid attack

6.4. Security for WI-FI wireless networks

By implementing these measures and keeping abreast of emerging threats, you can significantly improve the security of your Wi-Fi network.

6.4.1. Strong passwords

- **Create complex passwords:** combine upper- and lower-case letters, numbers and special characters.
- **Avoid personal information:** don't use birth dates, names or other easily guessable data.
- **Change passwords regularly:** update passwords regularly to reduce the risk of unauthorized access.

6.4.2. Robust Encryption

- **Use WPA3:** this is the most secure Wi-Fi encryption standard available.
- **Avoid WEP:** this obsolete encryption method is easily cracked.
- **Update firmware:** keep your router's firmware up to date to benefit from the latest security patches.

6.4.3. Network Isolation

- **Guest networks:** create separate networks for visitors to isolate them from your main network.
- **MAC address filtering:** restrict access to specific devices based on their MAC addresses, but be aware that this method can be bypassed.

6.4.4. Secure Connections

- **Use VPN:** use a VPN for added security, especially when using public Wi-Fi.
- **Avoid public Wi-Fi networks for sensitive activities:** avoid accessing banking services, e-mail or social networks on unsecured networks.

6.4.5. Regular Monitoring

- **Network analysis:** use tools to detect unauthorized devices on your network**.**

6.5. Securing digital media on the Internet (DRM 'Digital Right Management')

Digital Right Management (DRM) is a set of hardware and software technologies designed to control the way we use, modify and share content/information online. DRMs are also known as technological protection measures, as they aim to protect the copyright of technological content. The protection of protected works by various means to control or prevent the sharing of digital copies over computer/telecommunications networks. Protected data includes:

- Copyrighted multimedia content such as audio, video and images
- Copyrighted software, such as games, operating systems and applications
- Confidential documents, such as bank statements, company financial records
- Intellectual property assets such as product plans, diagrams, patents, data sheets

6.5.1. Techniques used

6.5.1.1. Restrictive licensing

The content provider creates a license that legally prevents users from using it for commercial or public distribution. The restrictive license makes users legally responsible for any unethical use of the image.

6.5.1.2. Digital trust infrastructure

Trust is rooted in the underlying digital infrastructure, maintaining a line of visibility and accountability over how, why and when content is shared. It gives users the autonomy to

play with content as they wish, while keeping the reins of control in the hands of the provider. It is extremely relevant for businesses.

6.5.1.3. One-way chopping

This is a cryptographic technique that prevents content manipulation.

It takes digital content as input and generates a final output message for user consumption. If the content is altered in any way, the output message will change, revealing that the content is not authentic. One-way hashing is used to verify digital content.

6.5.1.4. Secure communication protocols

Communication protocols such as SSL and TLS preserve the sanctity of information circulating on the Internet. They prevent tampering, ensuring that only secure, authentic content reaches the user. Secure communication protocols are an essential element of DRM, and must be part of the content technology stack.

6.5.1.5. Time-limited decryption keys

Encrypting data is an excellent way of keeping it out of immoral hands.

This is complemented by time-limited decryption keys that protect digital rights. The key would allow users to decrypt content for a specific period of time, as specified by the license/purchase conditions.

6.6. E-mail security, anti-spam mechanisms (statistical filtering mechanisms)

Email security is a term describing various procedures and techniques for protecting email accounts, content and communications from unauthorized access, loss or compromise. E-mail is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to share sensitive information, open attachments or click on hyperlinks that install malware on the victim's device.

6.6.1. Anti-spam mechanisms

6.6.1.1. Signature matching

Spammers send a copy of their spam message to every valid e-mail account they can find. Signature matching takes advantage of this by automatically deleting every copy of a spam message as soon as it recognizes it as spam. Providers of signature matching anti-

spam software maintain a large number of test accounts with Internet and e-mail service providers.

6.6.2. Heuristics

Each of the rules in a heuristic system is associated with a value. To determine whether a message is spam or not, the values of all the rules to which the message corresponds are added together. If the total value exceeds a threshold defined by the user or system administrator, the message will be filtered as spam. Simple heuristic filters use a small number of rules to search for obvious "bad" words and phrases, while more advanced filters use hundreds of rules and search for very complex features.

6.6.3. Bayesian filtering

Bayesian filters are one of the most recent technologies used to filter spam. The filters "learn" the difference between spam and non-spam, and continually update their knowledge to keep abreast of new spam. A Bayesian filter learns the difference between spam and non-spam by examining two large collections of e-mail messages. One collection contains spam messages received by a site, and the other collection contains non-spam messages received by the same site. The filter separates each message into individual words. Based on a comparison of the frequency of appearance of a given word in spam versus non-spam messages, the filter calculates the probability that a message containing that given word is spam.

6.7. Security in Web services

A Web service is software that makes itself available over the Internet, using a standardized XML messaging system. XML is used to encode all communications to a Web service. For example, a client calls a Web service by sending an XML message, then expects a corresponding XML response. As all communications are in XML, Web services are not tied to any operating system or programming language, i.e., C# can communicate with PHP, Windows applications can communicate with Linux applications.

6.7.1. XML-Signature

XML signatures are digital signatures designed for use in XML transactions. The standard defines a scheme for capturing the result of a digital signature operation applied to arbitrary (but often XML) data. XML signatures add authentication, data integrity and non-repudiation support to the data they sign. Unlike non-XML digital signature

standards, the XML signature has been designed to take advantage of both the Internet and XML.

Bibliography

[1] "2.4 Categories of Networks," Computer Networking concepts
. Accessed: Aug. 02, 2024. [Online]. Available: http://mucins.weebly.com/24-categories-of-networks.html

[2] "37-shiva sankar -Performance Metrics-c.pdf." Accessed: Aug. 02, 2024. [Online]. Available: https://www.ijarcce.com/upload/2013/march/37-shiva%20sankar%20-Performance%20Metrics-c.pdf

[3] "An Introduction to XML Digital Signatures." Accessed: Aug. 02, 2024. [Online]. Available: https://www.xml.com/pub/a/2001/08/08/xmldsig.html#sigs

[4] "Cellular Wireless Networks." Accessed: Aug. 02, 2024. [Online]. Available: https://www.tutorialspoint.com/wireless_communication/wireless_communication_cellular_networks.htm

[5] "Chapitre 3-RCSF | PDF | Échantillonnage (signal) | Réseau de capteurs sans fil," Scribd. Accessed: Aug. 02, 2024. [Online]. Available: https://fr.scribd.com/document/555004281/Chapitre-3-RCSF

[6] "Chapter 10: WLAN QoS Design — EasyQoS 1.6 latest documentation." Accessed: Aug. 02, 2024. [Online]. Available: https://easyqos-16.readthedocs.io/en/latest/chapter-10.html

[7] "Computer Networks | Electrical Engineering and Computer Science," MIT OpenCourseWare. Accessed: Aug. 02, 2024. [Online]. Available: https://ocw.mit.edu/courses/6-829-computer-networks-fall-2002/

[8] "cours_m2_2009.pdf." Accessed: Aug. 02, 2024. [Online]. Available: https://perso.telecom-paristech.fr/urien/cours_m2_2009.pdf

[9] "CSMA with Collision Avoidance (CSMA/CA)." Accessed: Aug. 02, 2024. [Online]. Available: https://www.tutorialspoint.com/csma-with-collision-avoidance-csma-ca

[10] "Difference Between 1G, 2G, 3G, 4G, 5G and 6G Technology." Accessed: Aug. 02, 2024. [Online]. Available: https://net-informations.com/q/diff/generations.html

[11] "Digital rights management | Copyright Protection, DRM Solutions & Strategies | Britannica." Accessed: Aug. 02, 2024. [Online]. Available: https://www.britannica.com/topic/digital-rights-management

[12] "Encountered a 404 error." Accessed: Aug. 02, 2024. [Online]. Available: https://nsnam.sourceforge.net/wiki/index.php/Main_Page

[13] "Everything You Should Know About Wi-Fi Security," Smallstep. Accessed: Aug. 02, 2024. [Online]. Available: https://www.smallstep.com/

[14] "Evolution of WiFi – Then and Now - Secure Networking For Enterprise." Accessed: Aug. 02, 2024. [Online]. Available: https://www.ray.life/evolution-of-wifi-then-and-now/

[15] "How Does Single Sign-On (SSO) Work? | OneLogin." Accessed: Aug. 02, 2024. [Online]. Available: https://www.onelogin.com/learn/how-single-sign-on-works

[16] "Multiple Access Protocols in Computer Network," GeeksforGeeks. Accessed: Aug. 02, 2024. [Online]. Available: https://www.geeksforgeeks.org/multiple-access-protocols-in-computer-network/

[17] "Network Simulator Tutorial." Accessed: Aug. 02, 2024. [Online]. Available: https://player.slideplayer.com/7/1716147/#

[18] “Overview of Wireless Metropolitan Area Network (WMAN),” GeeksforGeeks. Accessed: Aug. 02, 2024. [Online]. Available: https://www.geeksforgeeks.org/overview-of-wireless-metropolitan-area-network-wman/
[19] “Overview of Wireless Wide Area Network (WWAN),” GeeksforGeeks. Accessed: Aug. 02, 2024. [Online]. Available: https://www.geeksforgeeks.org/overview-of-wireless-wide-area-network-wwan/
[20] “Performance of Wireless Networks: Introduction to Wireless Networks - High Performance Browser Networking (O’Reilly),” High Performance Browser Networking. Accessed: Aug. 02, 2024. [Online]. Available: https://hpbn.co/introduction-to-wireless-networks/
[21] “QoS Requirements of Data > Quality of Service Design Overview | Cisco Press.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=357102&seqNum=3
[22] “Quality of service in mobile ad hoc networks.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.posterus.sk/?p=11789
[23] “réseau cellulaire systeme cellulaire cellular system définition.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.marche-public.fr/Terminologie/Entrees/reseau-cellulaire.htm
[24] “Réseaux de Capteurs Sans Fils - La solution TinyOS.” Accessed: Aug. 02, 2024. [Online]. Available: https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_37.html
[25] “Réseaux de Capteurs Sans Fils - LEACH: Low-Energy Adaptive Clustering Hierarchy.” Accessed: Aug. 02, 2024. [Online]. Available: https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_78.html
[26] “Réseaux de Capteurs Sans Fils - TEEN (Threshold sensitive Energy Efficient sensor Network protocol).” Accessed: Aug. 02, 2024. [Online]. Available: https://moodle.utc.fr/file.php/498/SupportWeb/co/Module_RCSF_79.html
[27] “Réseaux sans fil - Wireless Networks.” Accessed: Aug. 02, 2024. [Online]. Available: https://web.maths.unsw.edu.au/~lafaye/CCM/wireless/wlintro.htm
[28] “Sensor Networks: Definition, Operation & Relationship,” study.com. Accessed: Aug. 02, 2024. [Online]. Available: https://study.com/academy/lesson/sensor-networks-definition-operation-relationship.html
[29] “The Evolution of Cellular Networks | Engineers’ Insight | Avnet Abacus.” Accessed: Aug. 02, 2024. [Online]. Available: https://my.avnet.com/abacus/resources/article/the-evolution-of-cellular-networks/
[30] “Time Synchronization in Wireless Networks.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.cse.wustl.edu/~jain/cse574-06/ftp/time_sync/index.html#Section1.2
[31] “Tools | Computer Networks | Electrical Engineering and Computer Science,” MIT OpenCourseWare. Accessed: Aug. 02, 2024. [Online]. Available: https://ocw.mit.edu/courses/6-829-computer-networks-fall-2002/pages/tools/
[32] “Uses of WLAN.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.netlab.tkk.fi/opetus/s38118/s00/tyot/25/page4.shtml
[33] “vehicular ad-hoc network - an overview | ScienceDirect Topics.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/vehicular-ad-hoc-network

[34] “Waves and Electromagnetic Radiation.” Accessed: Aug. 02, 2024. [Online]. Available: https://saylordotorg.github.io/text_general-chemistry-principles-patterns-and-applications-v1.0/s10-01-waves-and-electromagnetic-radi.html
[35] “What Is Digital Rights Management? Definition, Benefits, and Best Practices - Spiceworks,” Spiceworks Inc. Accessed: Aug. 02, 2024. [Online]. Available: https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-digital-rights-management/
[36] “What is DNS cache poisoning? | DNS spoofing.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/
[37] “What Is Network Security?,” Cisco. Accessed: Aug. 02, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
[38] “What is Quality of Service (QoS) in Networking?,” Fortinet. Accessed: Aug. 02, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service
[39] “What is Widevine digital rights management (DRM) and why does it matter?,” Android Authority. Accessed: Aug. 02, 2024. [Online]. Available: https://www.androidauthority.com/widevine-explained-821935/
[40] “What Is Wi-Fi Security?,” Cisco. Accessed: Aug. 02, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html
[41] “Wi-Fi Security: WEP vs WPA or WPA2,” Wi-Fi Security: WEP vs WPA or WPA2. Accessed: Aug. 02, 2024. [Online]. Available: https://www.avast.com/c-wep-vs-wpa-or-wpa2
[42] “Wi-Fi - Quality of Service (QoS).” Accessed: Aug. 02, 2024. [Online]. Available: https://www.tutorialspoint.com/wi-fi/wifi_service_quality.htm
[43] “Wireless security,” *Wikipedia*. Jul. 10, 2024. Accessed: Aug. 02, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Wireless_security&oldid=1233609692
[44] “Wireless Sensor Network (WSN),” GeeksforGeeks. Accessed: Aug. 02, 2024. [Online]. Available: https://www.geeksforgeeks.org/wireless-sensor-network-wsn/
[45] “Wireless Sensor Network (WSN),” GeeksforGeeks. Accessed: Aug. 02, 2024. [Online]. Available: https://www.geeksforgeeks.org/wireless-sensor-network-wsn/
[46] “Wireless: What Does 802.11 Mean - GROK Knowledge Base.” Accessed: Aug. 02, 2024. [Online]. Available: https://networking.grok.lsu.edu/Article.aspx?articleid=5628
[47] “Wireless Wide Area Network - an overview | ScienceDirect Topics.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/wireless-wide-area-network
[48] “WLAN DCF vs PCF-Difference between DCF and PCF medium access.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.rfwireless-world.com/Terminology/WLAN-DCF-vs-PCF.html
[49] D. Bhattacharyya, T. Kim, and S. Pal, “A Comparative Study of Wireless Sensor Networks and Their Routing Protocols,” *Sensors (Basel)*, vol. 10, no. 12, pp. 10506–10523, Nov. 2010, doi: 10.3390/s101210506.

[50] D. E. Culler and PhD, “TinyOS: Operating System Design for Wireless Sensor Networks | Fierce Electronics.” Accessed: Aug. 02, 2024. [Online]. Available: https://www.fierceelectronics.com/iot-wireless/tinyos-operating-system-design-for-wireless-sensor-networks
[51] J. Garcia-Macias and J. Gomez, “MANET versus WSN,” in *Sensor Networks and Configuration: Fundamentals, Standards, Platforms, and Applications*, N. P. Mahalik, Ed., Berlin, Heidelberg: Springer, 2007, pp. 369–388. doi: 10.1007/3-540-37366-7_17.
[52] F. Goffinet, “Introduction aux technologies WLAN,” cisco.goffinet.org. Accessed: Aug. 02, 2024. [Online]. Available: https://cisco.goffinet.org/ccna/wlan/introduction-technologies-wlan/
[53] N. Gupta, A. Prakash, and R. Tripathi, “Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey,” *Vehicular Communications*, vol. 2, no. 4, pp. 223–237, Oct. 2015, doi: 10.1016/j.vehcom.2015.10.001.
[54] A. KOUIS, “Différence entre FDMA, TDMA et CDMA,” WayToLearnX. Accessed: Aug. 02, 2024. [Online]. Available: https://waytolearnx.com/2018/07/difference-entre-fdma-tdma-et-cdma.html
[55] M. Li, “Security in VANETs”.
[56] M. A. Matin, M. M. Islam, M. A. Matin, and M. M. Islam, “Overview of Wireless Sensor Network,” in *Wireless Sensor Networks - Technology and Protocols*, IntechOpen, 2012. doi: 10.5772/49376.
[57] O. O. Olakanmi, A. Dada, O. O. Olakanmi, and A. Dada, “Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions,” in *Wireless Mesh Networks - Security, Architectures and Protocols*, IntechOpen, 2020. doi: 10.5772/intechopen.84989.
[58] E. Raphaely, “Everything You Need To Know About Wireless Security,” SecureW2. Accessed: Aug. 02, 2024. [Online]. Available: https://www.securew2.com/blog/complete-guide-wi-fi-security
[59] resurge-admin, “Types of Wireless Technologies - Types of Wireless Network,” Connected Platforms. Accessed: Aug. 02, 2024. [Online]. Available: https://connectedplatforms.com.au/types-of-wireless-technologies/
[60] V. Richert, B. Issac, and N. Israr, “Implementation of a Modified Wireless Sensor Network MAC Protocol for Critical Environments,” *Wireless Communications and Mobile Computing*, vol. 2017, no. 1, p. 2801204, 2017, doi: 10.1155/2017/2801204.
[61] N. P. U. Rqzhao, X. Shen, N. P. U. Rqzhao, and X. Shen, “Broadcast Protocols for Wireless Sensor Networks,” in *Smart Wireless Sensor Networks*, IntechOpen, 2010. doi: 10.5772/13755.
[62] M. N. A. A. Salam, “Operating Systems for Wireless Sensor Networks”, Accessed: Aug. 02, 2024. [Online]. Available: https://www.academia.edu/23270300/Operating_Systems_for_Wireless_Sensor_Networks
[63] P. S. Sausen, M. A. Spohn, and A. Perkusich, “Broadcast routing in wireless sensor networks with dynamic power management and multi-coverage backbones,” *Information Sciences*, vol. 180, no. 5, pp. 653–663, Mar. 2010, doi: 10.1016/j.ins.2009.11.016.

[64] N. Shabbir, S. R. Hassan, N. Shabbir, and S. R. Hassan, “Routing Protocols for Wireless Sensor Networks (WSNs),” in *Wireless Sensor Networks - Insights and Innovations*, IntechOpen, 2017. doi: 10.5772/intechopen.70208.
[65] A. M. Vegni, M. Biagi, R. Cusani, A. M. Vegni, M. Biagi, and R. Cusani, “Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks,” in *Vehicular Technologies - Deployment and Applications*, IntechOpen, 2013. doi: 10.5772/55492.
[66] A. Yasser, M. Zorkany, and N. Abdel Kader, “VANET routing protocol for V2V implementation: A suitable solution for developing countries,” *Cogent Engineering*, vol. 4, no. 1, p. 1362802, Jan. 2017, doi: 10.1080/23311916.2017.1362802.