A PRIMER ON
WIRELESS TECHNOLOGY AND IOT BASICS

Mamatha Balachandra
Balachandra Muniyal

Bentham Books

A Primer on Wireless Technology and IoT Basics

Authored by

Mamatha Balachandra & Balachandra Muniyal
School of Computer Engineering
Manipal Institute of Technology
Manipal Academy of Higher Education
Udupi, Karnataka, India

A Primer on Wireless Technology and IoT Basics

Authors: Mamatha Balachandra and Balachandra Muniyal

ISBN (Online): 979-8-89881-012-2

ISBN (Print): 979-8-89881-013-9

ISBN (Paperback): 979-8-89881-014-6

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2025.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

BENTHAM SCIENCE

CONTENTS

FOREWORD i

PREFACE ii

CHAPTER 1 INTRODUCTION TO WIRELESS NETWORKS 1
- **INTRODUCTION** 1
- **EVOLUTION OF WIRELESS NETWORKS** 3
- **WIRELESS NETWORK CHALLENGES** 4
  - Power Consumption 4
  - Efficient Spectrum Usage 4
  - Integrated Customer Services 4
  - Network Support for user Mobility 4
  - QoS (Quality of Service) 4
  - Connectivity and Coverage 5
  - Fading 5
  - Security 5
- **ELECTROMAGNETIC SPECTRUM** 5
- **WIRELESS TRANSMISSION AND FREQUENCY SPECTRUM** 6
- **MODULATION TECHNIQUES** 8
  - Analog Modulation Techniques 9
  - Amplitude Modulation 9
  - Frequency Modulation 9
  - Digital Modulation Techniques 11
- **SPECTRUM ALLOCATION TECHNIQUES** 11
  - Frequency Division Multiple Access (FDMA) 11
  - Time Division Multiple Access (TDMA) 11
  - Code Division Multiple Access (CDMA) 13
- **CELLULAR CONCEPT** 14
  - Frequency Reuse 15
  - Allocations 16
  - Types of Wireless Networks 17
  - Integration of Wireless Networks with IoT (Internet of Things) 17
- **CONCLUDING REMARKS** 18
- **EXERCISES** 18
- **REFERENCES** 19

CHAPTER 2 CELLULAR NETWORKS 20
- **INTRODUCTION** 20
- **1G: ANALOG CELLULAR SYSTEM** 21
  - Advanced Mobile Phone System 21
  - AMPS Channels 22
  - Network Operations 22
  - Initialization 23
- **2G: CELLULAR SYSTEMS** 23
  - Digital Advanced Mobile Phone System (DAMPS) 23
  - DAMPS Channels 24
- **2G: GSM** 24
- **GSM ARCHITECTURE AND MOBILITY MANAGEMENT** 25
  - Mobile Station (MS) 25
  - Base Station Subsystem (BSS) 26
  - Network Subsystem 27

Equipment Identity Register (EIR) 27
Public Switched Telephone Networks (PSTN) 27
GSM Authentication and Security 27
GSM FRAMES AND MULTI-FRAMES 28
GSM APPLICATIONS 29
MOBILITY MANAGEMENT IN GSM 30
GSM HANDOFF 31
3G CELLULAR NETWORKS 31
CDMA 2000 31
Evolution 31
Working 32
CDMA APPLICATIONS 33
WIDEBAND CODE DIVISION MULTIPLE ACCESS (WCDMA) 34
UMTS TRANSMISSION NETWORKS 35
4G CELLULAR NETWORKS 36
4G Wireless Standards 37
3G *Versus* 4G 37
System Interoperability 38
Multimode Devices Architecture 38
Overlay Network Architecture 38
Terminal Bandwidth and Battery Life 40
Varying Quality of Bandwidth for Wireless Access Based on Geographic Location 40
OFDM 40
CONCLUDING REMARKS 42
EXERCISES 42
REFERENCES 42

CHAPTER 3 FIXED WIRELESS NETWORKS 43
INTRODUCTION 43
Important Parameters of WLAN 44
WLAN Advantages 45
IEEE 802.11a, b, and g 46
802.11 Medium Access Control (MAC) sublayer of Wireless LAN 47
Hidden Terminal Problem 47
Exposed Terminal Problem 48
WLAN Applications 49
WiMAX 50
Comparison of Traditional Wired Networks with Fixed Wireless Networks 51
Sample use Case Explaining the Deployment of Fixed Wireless Networks 51
CONCLUDING REMARKS 52
EXERCISES 52
REFERENCES 53

CHAPTER 4 MOBILE AD HOC NETWORKS 54
INTRODUCTION 54
MANET Characteristics 54
MANET Challenges 55
MAC Protocols in MANETs 55
Contention-based MAC Protocols 56
Contention-based MAC Protocols with Reservation Mechanism 57
Contention-based MAC Protocols with a Scheduling Mechanism 57
Problem of using CSMA in MANETs 57

ROUTING IN AD HOC NETWORKS 58
Proactive Routing 60
Reactive Routing 60
The Destination Sequence Distance Vector (DSDV) Routing Protocol 61
Wireless Routing Protocol (WRP) 62
The Dynamic Source Routing (DSR) Protocol 62
The Ad Hoc On-demand Distance Vector Routing (AODV) Protocol 63
VANETs (IEEE 802.11p) 65
CONCLUDING REMARKS 66
EXERCISES 66
REFERENCES 66

CHAPTER 5 WIRELESS PERSONAL AREA NETWORK 67
INTRODUCTION 67
Bluetooth (IEEE 802.15.4) 68
Bluetooth Protocol Stack 70
Bluetooth Applications 72
Bluetooth Security 72
Connecting to Devices via Bluetooth and Transferring Files 73
ZigBee 73
ZigBee Systems Architecture 73
ZigBee Applications 74
ZigBee versus Bluetooth 75
Wireless Sensor Networks 75
Wireless Sensor Network (WSN) Protocol Stack 76
Wireless Image Sensor Network 76
CONCLUDING REMARKS 77
EXERCISES 77
REFERENCES 77

CHAPTER 6 WIRELESS SENSOR NETWORKS 78
INTRODUCTION 78
Why do we need a Sensor Network? What is the Difference between a Sensor and a WSN? 79
Classification of WSN 79
Basic Architecture of WSN 80
Constraints on the Sensor Nodes in WSN 80
Challenges to be Faced in Building Sensor Networks 80
Sensor Networks Deployment 81
To Understand more about the Coverage and Connectivity 82
Coverage Problem in Static WSN 83
Applications of WSN 85
CONCLUDING REMARKS 90
EXERCISES 90
REFERENCES 90

CHAPTER 7 FUNDAMENTALS OF 5G NETWORKS 92
INTRODUCTION 92
5G Internet 93
Better Signals 93
Efficient Transmission 93
5G Working 94
MIMO (Multiple Input Multiple Output) Technology 95

5G Use Cases 97
5G and IoT Integration 98
Security Challenges in 5G Networks 98
CONCLUDING REMARKS 99
EXERCISES 99
REFERENCES 99

CHAPTER 8 INTERNET OF THINGS 101
INTRODUCTION 101
Equation of IoT 102
Implementation Aspects of IoT 103
Protocols in IoT 106
Advancements in IoT 115
About Use Cases and Example Use Case 117
Example Prototype: IoT Indoor Localization Using Bluetooth Low Energy (BLE) 119
Data Handling and Analysis for IoT 119
Data Handling Technologies in IoT 122
Cloud Computing 122
Data Centers 122
Real-World IoT Applications 123
Agricultural Internet of Things and Decision Support for Precision Smart Farming: A Use Case 123
CONCLUDING REMARKS 124
EXERCISES 124
REFERENCES 125

CHAPTER 9 FUNDAMENTALS OF 6G NETWORKS 127
INTRODUCTION 127
Comparison of 6G with 4G and 5G 128
6G ELECTROMAGNETIC SPECTRUM 128
6G CHALLENGES 129
ARCHITECTURE OF 6G 130
POTENTIAL TECHNOLOGIES 131
RECENT RESEARCH ON 6G AND AI 132
CONCLUDING REMARKS 132
EXERCISES 133
REFERENCES 133

SUBJECT INDEX 134

FOREWORD

Wireless Communication introduced a paradigm shift in long-distance communication. With the success of landline telephone networks as well as computer/data networks, the need for mobile telephone networks was felt. This requirement was materialized with the commercialization of cellular communication networks. It was realized that wireless networks without infrastructure are necessarily required in many applications, including military communications. Further, the success of cellular networks led to other wireless sensor networks. Short and medium-range wireless networks, such as WiFi networks and wireless personal area networks, were materialized, providing ubiquitous communication. This book starts with the basics of wireless networks, progressing toward a detailed explanation of cellular networks, fixed wireless networks, and mobile ad hoc networks. Further, wireless personal area networks and wireless sensor networks are discussed in some detail. Also, chapters on IP multimedia services, fundamentals of 5G networks, and the Internet of Things are included for completeness.

The author's presentation style is excellent. She strikes a balance between coverage of topics and depth of presentation. I wholeheartedly congratulate Dr. Mamatha Balachandra for the conception and execution of the book on wireless networks with such coverage, clarity, and presentation style. This book is a very timely and comprehensive contribution to wireless network research literature.

G. Rama Murthy
Mahindra University Bahadurpally
Hyderabad-500043, Telangana
India

PREFACE

Wireless networks are growing day by day in almost all parts of human life. People cannot survive without them even for their household work, for example, booking tickets, getting appointments with doctors, paying bills, purchasing items, *etc*., from anywhere at any point in time. Wireless networks are useful in reducing networking costs in several cases. As and when their usage increases, there exist several challenges to be faced while using wireless technology. This book gives a basic idea about the evolution and growth of wireless technology, starting from very basic wireless technologies such as GSM and GPRS to WLANs, WPAN, WMANs, cellular networks (from 1G to 5G), and the Internet of Things (IoT).

Nowadays, the Internet of Things is one of the very hot technologies across the globe. All types of organizations, government, private, and industry, are involved in the different aspects, such as implementation, business, and research on IoT. Currently, a lot of investments are being made in almost all these organizations in the development of the Internet of Things. The applications of IoT are broadly in areas like business, healthcare, biometric and facial recognition, inventory tracking, and so on. IoT is used most commonly in smart cities, smart health, smart agriculture, supply chain control, forest fire detection, air pollution detection, *etc.*

The Introduction section of Chapter 1 gives the basics of wireless networks, followed by the evolution of wireless networks, the next wireless network challenges, and various types of wireless networks. Chapter 2 presents generations of cellular networks, *i.e*., 1G, 2G, 3G, and 4G, in terms of their working, categories, and applications. An overview of WLAN in terms of infrastructure and WLAN technology based on the IEEE 802.11 standard is introduced in Chapter 3. Chapter 4 provides mobile ad hoc network (MANET) challenges, protocols, and various routing algorithms in MANETs. An overview of WPAN in terms of various technologies used, such as ZigBee, Bluetooth, WSN, WISN, *etc*., is given in Chapter 5. Chapter 6 presents the overview of WSN, categories of WSN, WSN architecture, and WSN coverage and connectivity. An overview of IMS (IP Multimedia Subsystem), the technology that merged with the cellular world, is provided in terms of its architecture, applications, and developing services within the IMS in Chapter 7. An overview of 5G technology in terms of its characteristics, working, and Massive MIMO technology is discussed in Chapter 8. Chapter 9 gives the basics of IoT, IoT connectivity, and IoT use cases, along with the working of sample use cases and important protocols for establishing the connectivity between the IoT devices and the Internet.

Mamatha Balachandra & Balachandra Muniyal
School of Computer Engineering
Manipal Institute of Technology
Manipal Academy of Higher Education
Udupi, Karnataka, India

CHAPTER 1

Introduction to Wireless Networks

Abstract: Wireless Network refers to computer networks without wired connections wherein nodes communicate with each other using radio frequency connections. One of the key benefits of wireless networks is that they can be easily deployed anytime and anywhere for applications such as homes, industry automation, military, agriculture, business, *etc*. This chapter discusses the basics of wireless networks, followed by wireless network evolution, wireless network challenges, the type of wireless network, and how wireless networks are integrated with the Internet of Things (IoT).

Keywords: Challenges, Evolution, IoT, Radio, Wireless networks.

INTRODUCTION

A computer network is a collection of two or more connected computers. Through these networks, people can share data as well as hardware resources and communicate with each other. Computer networks are broadly categorized under two headings: Wired and Wireless networks.

The basic component required for building networks is at least two computers. When we say computer, it need not be just a computer; instead, it can be even a small computing device. We can also have wireless Ad hoc networks, where each computing device is a small microcontroller, sensor, or other device. The other requirement is that there should be a Network Interface Card (NIC) in each computer, a connection medium, which can be a wireless medium, and a network operating system software that controls all of these.

In a wired scenario, a hub or switch is used to connect computers in the network. Here, the responsibility of the hub is to forward data packets from one computer to another. In wireless networks, Mobile Switching Centers act like central hubs. Hubs forward any data packet from one workstation to another [1].

We can use hubs to connect to access, wherein we can connect to LANs. Another important networking component is the router. The responsibility of the router is to route the packet from the source node to the destination node, which also maintains a routing table to determine the next hop. The entire data is divided into

Mamatha Balachandra & Balachandra Muniyal

packets, which travel in the most efficient paths. It is the responsibility of the router to transmit the packet. Routers are also used to connect any network in a wide area network.

The next device in a wireless network is the access point, which performs the operations like the hub. The access point avoids a wired connection. Some access points have roaming functionality. Access points can connect a wired network to a wireless network so that access points help get service from a wired network to a wireless network. Access points help extend or add more devices to the network. They act like a bridge between wired Ethernet or fast Ethernet Networks. They are very useful in adding more computers to the lab. A sample example wireless network is shown in Fig. (**1**).

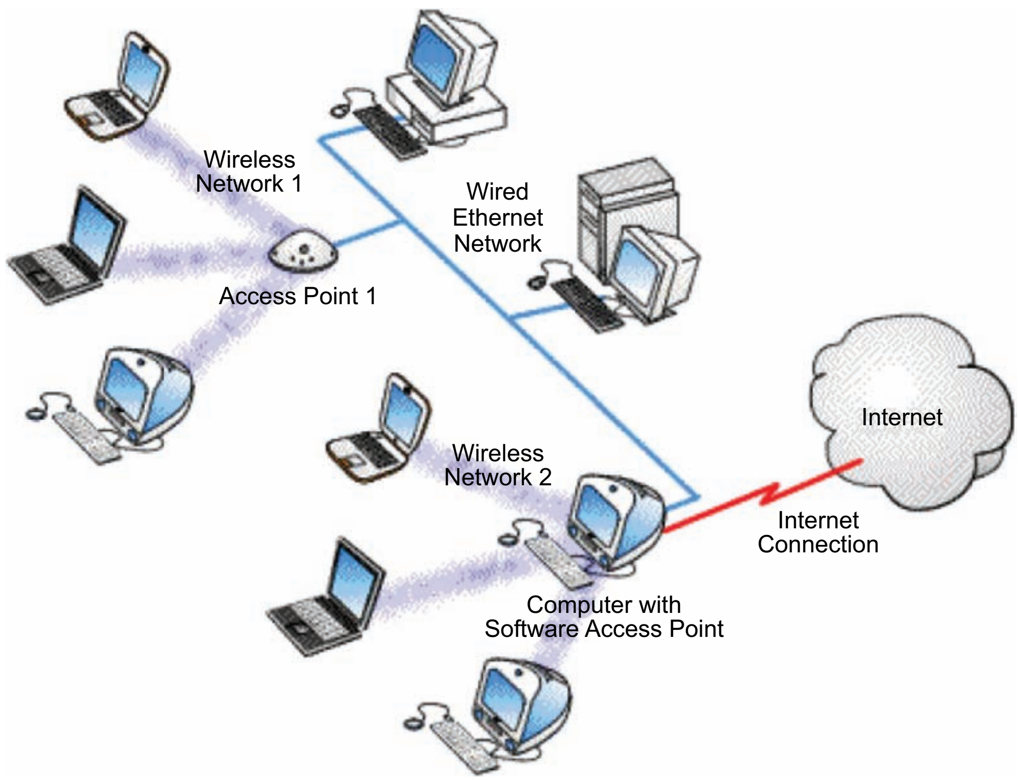

Fig. (1). Sample Wireless Network.

Wireless LAN (WLAN) is an alternative to wired LAN. Using RF technology, users of WLAN can access information over the air without the need to establish a physical connection. By using WLAN, anybody can access shared information without plugging in and looking for a place to plug in. It is a huge advantage of WLAN.

Wireless networks are growing day by day in almost all parts of human life. People cannot survive without them, even for their household work, for example, booking tickets, getting appointments with doctors, paying bills, purchasing items, *etc*., from anywhere at any point in time.

One of the reasons for using wireless networks in our day-to-day real-life applications is due to their cost-effectiveness. As and when their usage increases, there exist several challenges to be faced while using wireless technology.

EVOLUTION OF WIRELESS NETWORKS

In the first-generation wireless technology, analog ARMs were used. These are cordless telephones (CT) with different standards across the globe. CT1, CT2, and CT3 were the various cordless telephone standards. The specialty of the 1G network is that they were analog and used frequency division multiplexing with limited roaming. There was no real standard across the globe. The MSC was very big. The progress of wireless networks was happening in three geographical regions, which were Europe, the US, and Japan.

In the second-generation GSM technology, GSM 800 and GSM 900 were developed. The specialty of 2G is it uses digital and Time Division Multiplexing Access based primarily on more roaming with better performance and smart billing. Other features are mobile-to-mobile calls, power-controlled Dynamic channel allocation, mobile-assisted handoff, *etc*. This is more robust compared to 1G systems. GSM is one of the most successful wireless technologies that is used even now across the world. Japan came up with PDC in the second generation. The US went towards digital arms, then IS 54, PCS900, and CDMA-based IS95. Europe moved towards GSM 900. GPRS and Edge are moving towards the 3G system.

In 3G, the basic philosophy is one world standard. Cordless and wireless technology converged. Wireless phones are connected to IP, *i.e*., we can make VOIP calls through cellular phones. The same device acts like a cordless phone inside a home or a cellular phone outside the home, and if we are near an access point, we can make VOIP. This is how the 3G network has emerged. 3G has a combination of various features with better voice quality and video quality. 3G is not only about higher speed but also about a greater number of services with better Quality of Service (QoS) and mobility.

CHAPTER 2

Cellular Networks

Abstract: A cellular network refers to a mobile network wherein nodes distributed across long distances communicate with each other using radio frequency connections. Cellular wireless networks divide large geographic areas into sections or cells, each served by at least one transceiver. In this chapter, various generations of cellular networks, 1G, 2G, 3G, and 4G, in terms of their working, categories, and applications are discussed. Also, technologies that are used, especially in 3G and 4G cellular networks such as WCDMA and OFDM, are explained.

Keywords: 1G, 2G, 3G, 4G, CDMA, GPRS, GSM, OFDM, UMTS, WCDMA.

INTRODUCTION

Today, a cellular network is a common man's technology. The wireless network is not equal to the cellular network, but it is much bigger. Cellular technology happens to be the most dominant technology. Cellular technology is much more than WPAN (Wireless Personal Area Network) or WLAN (Wireless Local Area Network). A cellular network is a WWAN (Wireless Wide Area Network) that covers large geographical areas, which is much bigger than WPAN and WLAN.

The base stations are every 500 meters to cover the wireless range. Unfortunately, the range is good, but the interference is bad, and we need to have the proper balance between interference and the range.

Cellular technology is a licensed technology, which means we cannot transmit through cellular networks without licensed bands. Before the smartphones that we are using now, there were several versions of phones such as Motorola Micro Tac (1986), Nokia 101 (1992), Motorola StarTAC(1996), Blackberry 5810(2002), Apple Phone (2007), iPhone (2012), *etc*. This is the evolution that happened in terms of handsets. But in terms of functionality, we can categorize them into 1G, 2G, 3G, 4G, 5G, and so on. Each cellular network generation is the improved version of the previous generation in terms of data rate, access technology, bandwidth, range of coverage, *etc*.

Mamatha Balachandra & Balachandra Muniyal

1G: ANALOG CELLULAR SYSTEM

In 1946, the first telephone system, which is known as MTS (Mobile Telephone System) was introduced. They had several disadvantages, which are mentioned below:

a. Transceivers were very huge, and vehicles were used to carry them.
b. Inefficient usage of the Spectrum.
c. Manual call switching.

The major difference between MTS and 1G cellular systems was that 1G made use of the cellular concept. The cellular concept greatly improves spectrum usage. The 1G cellular phone was analog, *i.e.*, it made use of analog signaling for communicating. Due to this, the following problems arose:

i. Encryption is not possible: There is no encryption of the traffic in a 1G system. So, voice calls through such networks are susceptible to interception, causing them to be vulnerable to eavesdropping. Also, there is a possibility of revealing user identification numbers, thus placing illegal calls by listening to the channels.
ii. Inferior call quality: Analog signaling for communication results in inferior call quality as it is easily degraded by interferences.
iii. Spectrum inefficiency: Since each Radio Frequency (RF) carrier is dedicated to a single user in the case of analog signaling, irrespective of whether the user is active or not, it results in inefficient spectrum utilization.

Analog systems have been deployed worldwide during the first generation of cellular systems. In the United States, the Analog Mobile Telephone System (AMTS) was developed in 1982, offering voice transmission. Advanced Mobile Phone System (AMPS) was developed during the early 1980s by Bell Laboratories. It was designed to provide mobile telephone traffic services *via* the number of 30KHz channels between base stations and mobile stations of each call. All these 30KHz channels were used to carry voice traffic [1].

Advanced Mobile Phone System

During the 1980s, the first allocation of bandwidth for AMPS was made by the Federal Communication Commission (FCC) in order to test systems in the Chicago area. The allocation bandwidth was in the 800MHz part of the spectrum. This is because above 800MHz was a very densely used allocation of frequencies in the bands of AMPS, which caused severe attenuation due to path loss or fading. Also, the 800MHz band was a relatively unused band.

AMPS Channels

AMPS had two sets of channels: A (1 to 333) and B (334 to 666). Channels 313 to 333 and 334 to 354 are the control channels of channels A and B, respectively. Each operator has 21 control channels and 312 voice channels.

Traffic channels are 30KHz analog FM channels to serve the voice traffic. The main traffic channels are the Forward Voice Channel (FVC) and Reverse Voice Channel (RVC), carrying voice traffic from the Base Station (BS) to the Mobile Station (MS) and from MS to BS.

Control channels (CC) carry digital signaling and are used to coordinate medium access of mobile stations. The main control channels are the Forward Control Channel (FCC) and the Reverse Control Channel (RCC).

Supervisory Audio Tone (SAT) is sent on the voice channel to enable MSs and BSs to process information on the quality of the link and to ensure link continuity.

The signaling tone of AMPS is used to send four signals: (i) A *request to send* whose task is to allow the user to enter more data, (ii) an *alert signal,* which is continuously sent until the user of MS answers the call, (iii) a *discount call* sent by MS over RVC, which is to indicate the termination of the call, and (iv) the handoff of the current MS to another BS is done by sending handoff information by MS in response to network request [2].

Network Operations

a. Electronic Serial Number (ESN): A string of 32 bits uniquely identifies AMPS MS. This number is set by the MS manufacturer and is burned into ROM to prevent unauthorized changes of the number. If someone tries to rewrite ESN, MS will become inoperable. The 18-bit Manufacturers code (MFR) of ESN uniquely identifies each manufacturer; another 6 bits remain unused, and the next 8 bits represent the serial number. If more and more MSs are manufactured, then additional serial numbers in combination with the same MFR can be used to identify new sets of MSs.
b. System Identification Number (SID): This is a 15-bit number that indicates the AMPS network. This is transmitted by BS to MS.
c. Mobile Identification Number (MIN): It is a 34-bit string that is derived from 10 digit telephone number (24 bits from local code + 10 bits from global code).

CHAPTER 3

Fixed Wireless Networks

Abstract: Fixed Wireless Networks are used to establish communication between two fixed locations *via* radio link or some other wireless means. Wireless Local Area Network (WLAN) is one of the popular Fixed Wireless Networks that can provide high-speed Internet access over wide area networks. WLAN can be configured into either infra-structured networks or an Ad hoc network. This chapter introduces WLAN technology based on the IEEE 802.11 standard. For wireless broadband services, IEEE 802.16 or WiMAX standards are introduced. Comparison of traditional wired networks with fixed wireless networks is also discussed based on important aspects such as speed, bandwidth, installation, cost, coverage, maintenance, *etc*. A sample use case that gives a basic idea about the creation of a Fixed Wireless Network is also illustrated.

Keywords: AD HOC, IEEE 802.11, IEEE 802.16, WLAN.

INTRODUCTION

Let us discuss the need for fixed wireless networks. Due to the advancement in VLSI (Very Large-Scale Integration) technology recently, the number of portable battery-operated equipment such as laptops, cellphones, PDA (Personal Digital Assistants), and palmtops has increased tremendously. These low-cost portable equipment are the driving force behind fixed wireless networks. Moreover, they have a lot of benefits; one of them is mobility. Due to this, people can communicate with each other while traveling and can attend conferences or meetings remotely from anywhere. Also, they have other benefits such as simple installation compared to their wired counterpart, minimal ownership cost, and easy scalability. One of the popular fixed wireless networks is WLAN.

WLAN offers several limitations as well as challenges. They are listed below:

i. Unreliable due to interference and noise: As communication happens through unguided media, unlike wired counterparts, there may be other devices communicating at the same frequency band that will interfere with the signal, which leads to low reliability due to the susceptibility of radio transmissions.
ii. Problem of fading: Signals can come through multiple paths that lead to fading due to fluctuations.

Mamatha Balachandra & Balachandra Muniyal

iii. Vulnerability to eavesdropping leads to security problems: Whenever someone is transmitting something through wireless media while broadcasting, unauthorized users can make improper use of it.
iv. Smaller data rate: The usage of spread spectrum in wireless networks leads to smaller data rates compared to wired LAN data rates.

The WLAN concept is simple. WLAN makes use of important standards, which are IEEE 802.11. Among various categories of protocols under IEEE 802.11, IEEE 802.11b is the most popular standard used nowadays. Like any other LAN technology, it consists of two layers: The physical layer and the data link layer. The Data Link Layer has two sub-layers: the Medium Access control layer and the Logical link control layer. IEEE 802.11b layered architecture is shown in Fig. (**1**).

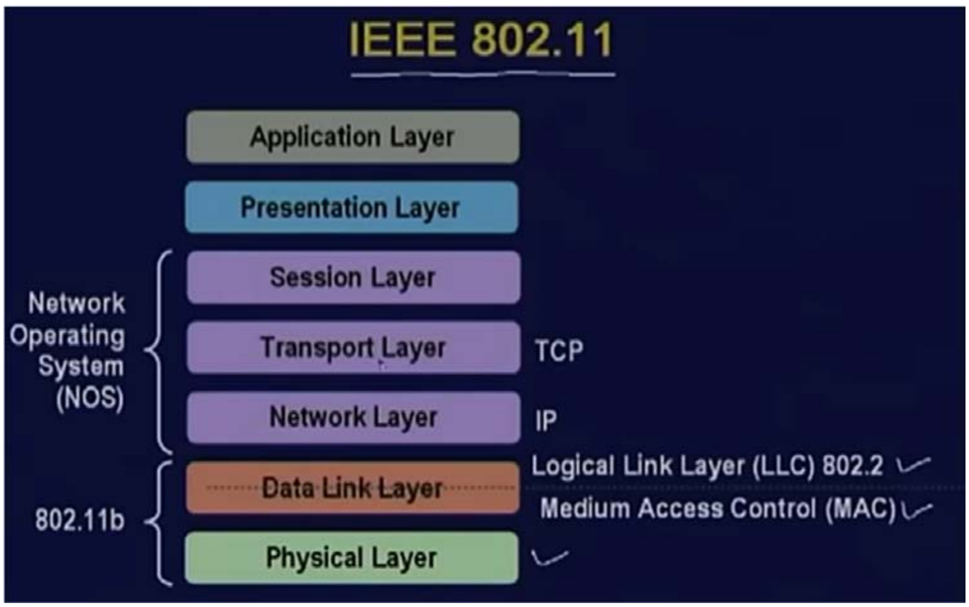

Fig. (1). IEEE 802.11 Layered architecture.

So essentially, the functionality of the bottom two layers, *i.e.*, the Physical layer and Medium Access layer, will be different in Wireless LAN, and the functionality of the upper layers, like TCP, IP, *etc.*, remains the same [1].

Important Parameters of WLAN

WLAN is characterized in terms of three important parameters: Topology, Transmission media, and Medium Access control techniques.

i. Transmission Media: Three different types of physical media are called Spread spectrum radio used in the 2.4GHz (2400 to 2483 MHz) ISM band, which is very popular and used by most household equipment. Spread Spectrum has 2 different approaches. They are FHSS (Frequency-hopping spread spectrum) and DSSS (Direct Sequence Spread Spectrum). The third approach is based on the infrared signal in the near visible range of 850 nanometers to 950 nanometers.
ii. Topology: IEEE 802.11 supports 2 types of BSS (Basic Service Sets). They are Ad hoc networks without access points and Infrastructure BSSs with access points.
iii. Medium Access Control: One of the challenges associated with Wireless LAN is that it is less reliable as it is more prone to interference.

WLAN Advantages

In the last two decades, the wired version of LAN has large-scale deployment and is widely used all over the globe. Until recently, wireless versions of LANs were not popular due to reasons such as low data rate, high cost, licensing requirements, and occupational safety concerns. This situation has changed significantly in the last couple of years.

WLAN has plenty of advantages. Important among them are listed below:

1. **Reduced Cost and Portable Equipment:** The equipment cost that is required for WLAN set-up has been reduced a lot due to the technological enhancements.
2. **Mobility:** With Wireless LAN, people can connect from any location without making use of cables and can attend meetings or conference calls even during traveling; the usage of WLAN has increased tremendously.
3. **Installation Speed and Simplicity:** Installation of Wireless LANs happens very easily and quickly compared to their wired counterpart. With wireless installation, there is no need for wiring for every workstation. This installation makes wireless LANs inherently flexible. Even the movement of the workstation can be done easily.
4. **Installation Flexibility:** Since wireless LAN can be installed anywhere, for example, in places where natural disasters have occurred, such as floods or earthquakes, there is a high level of flexibility and portability with this type of network.
5. **Reduced Cost of Ownership:** Even though the initial installation might require more expenditure on wireless connectivity for its hardware, it is surveyed that the overall installation expenses and life cycle costs can be significantly lower.

CHAPTER 4

Mobile Ad hoc Networks

Abstract: Mobile Ad hoc Network (MANET) is a category of Wireless Ad hoc Network. In MANET, topology keeps changing very frequently due to the mobility of nodes in the network. MANET faces a lot of challenges, such as the environment itself being decentralized, the medium being more error-prone, routing overhead, nodes operating with limited energy, and so on. There exist separate routing algorithms for Ad hoc networks, such as DSDV, DSR, AODV, CGSR, and WRP. VANET (Vehicular Ad hoc Network) is a special type of Intelligent Transport System (ITS), where the mobile nodes are cars, two-wheelers, trucks, buses, *etc*.

Keywords: AODV, CGSR, Challenges, DSDV, DSR, IEEE 802.11p, MANET, Mobility, VANET, WRP.

INTRODUCTION

Wireless Ad hoc networks are a broad class of networks. It is classified into pure wireless ad hoc networks, Mobile Ad hoc Networks (MANETs), Vehicular Ad hoc Networks(VANETs), and Wireless Sensor Networks (WSNs). In MANETs, some or all the nodes of the network are mobile or movable. Some of the important properties of MANETs are self-configure, self-heal, self-optimize, and self-protect. In MANETs, there are frequent link changes, which consequently lead to dynamic topological changes. Each node in MANETs acts as a router to forward the packets to other nodes in the network. Traditional routing protocols, which are used in wired networks, cannot be used with MANETs. IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication system. To work with VANETs, an enhanced version of IEEE 802.11p is developed.

MANET Characteristics

a. **Wireless:** Nodes in MANET operate in wireless media or wireless environment.
b. **Mobile:** Nodes are mobile in nature.
c. **No Structure:** There is no fixed structure for MANET. Topology keeps changing due to node mobility.

Mamatha Balachandra & Balachandra Muniyal

d. **Heterogeneous:** Nodes may be of different specifications.
e. **Autonomous Behavior:** MANETs can operate on their own, or they survive on their own whenever there is some kind of abnormality in the network.
f. **Dynamic Network Topology:** This means each node in the network can be joined or separated from the **network** anytime and anywhere.
g. **Energy-constrained:** Each node in MANET operates with a battery, so nodes have limited energy.

MANET Challenges

There exist some challenges in enabling the MANETs:

a. **Limited Bandwidth:** MANETs operate in the wireless medium. The availability of radio frequency bands is limited in the wireless medium.
b. **Dynamic Topology:** Due to the mobility of the nodes, topology keeps changing very frequently.
c. **Routing Overhead:** This is due to the periodic movement of nodes in the network. As and when nodes move, there is a routing overhead while discovering the new path to reach the destination and also maintaining the new routing information at every node.
d. **Hidden Terminal Problem:** In the case of MANETs, wireless nodes have transmission ranges, and not all stations are in the same range as each other, causing hidden station problems.
e. **Security Threats:** Due to the presence of features like open wireless medium, dynamic topology MANET is prone to security threats.
f. **Packet Losses Due to Transmission:** This is one of the significant problems that happen in the MANET while routing. This link breakage causes **packet loss** and **latency** problems in the network, and it degrades the performance. Each node in **MANET** acts both as a host and as a router.

MAC Protocols in MANETs

MAC protocol is essentially a set of rules or procedures that allow the efficient use of shared wireless medium by multiple users. In MANET, there may be a set of wireless nodes in the network that want to communicate with one another with multiple wireless paths. What is required here is to provide a mechanism in which these nodes will communicate with each other through a shared medium. So, MAC protocol in an Ad hoc network will help in doing so.

MAC protocol is concerned with per-link communication. This means that the nodes that are within the range of each other can communicate. MAC protocol needs some revision before using MANETs due to the following issues:

a. **Lack of Centralized Control:** Here the nodes do not have a complete view of the network, and there is a requirement for complete coordination to avoid collision between the packets sent by nodes.
b. **Nodes are Mobile:** Due to the movement of nodes in MANET, topology keeps changing.
c. **Nodes are Resource Constraints:** Due to limited energy available at the nodes in MANETs, we cannot run complicated algorithms.
d. **Wireless Channels are not Reliable:** Wireless channels are more prone to errors compared to their wired counterparts. These channels suffer from path loss, fading, and interference.
e. **Have Limited Channel Bandwidth:** MANETs have limited channel bandwidth. So, different nodes should share the bandwidth among them for communication.

MAC protocols are broadly classified under two headings:

Contention-based MAC Protocols

Here, the nodes are about to contend or compete to transmit the data to one or other nodes in the network, and there are no QoS guarantees. This means there is no guaranteed access to the channel. These protocols are further classified into sender-initiated protocols and receiver-initiated protocols.

i. Sender-initiated protocols: In sender-initiated protocols, more than one control packet is needed. So basically, the sender, instead of directly sending the data, sends the RTS/CTS(Request to send/Clear to send). Sender-initiated protocols are classified into Single-channel protocols and Multiple-channel protocols.

Examples of Single channel protocols: Multiple Access with Collision Avoidance (MACA) and Multiple Access with Collision Avoidance for Wireless (MACAW).

Examples of Multi-channel protocols: BTMA (Busy Tone Multiple Access) and DBTMA (Dual Busy Tone Multiple Access).

ii. Receiver-initiated protocols: In receiver-initiated protocols, the receiver initially does not know whether the sender has some data to send. The only way to know this is by periodically polling the sender. So here, only one control packet is used. The protocols under this category are Multiple Access Collision Avoidance By Invitation (MACA-BI) and Receiver-Initiated Busy-Tone Multiple Access (RI-BTMA).

CHAPTER 5

Wireless Personal Area Network

Abstract: Wireless Personal Area Network (WPAN) or IEEE 802.15.4 standard defines the medium access control and physical layer specifications for low data rate wireless connectivity, interconnecting fixed or moving portable devices with low or no battery. A WPAN transmits data among devices such as laptops, smartphones, tablets, and personal digital assistants. IEEE 802.15.4 is a base on which several standards, such as ZigBee, Bluetooth, WSN, WISN, *etc*., are built and can be used based on various applications.

Keywords: Bluetooth, WISN, WSN, WPAN, ZigBee.

INTRODUCTION

Wireless personal area networks (WPANs) are used by several technologies such as ZigBee, Bluetooth, 6LowPAN, Wireless HART, WSN, WISN, MiWi, ISA 100.11a *etc*., as shown in Fig. (**1**). If we purchase any of the products of IEEE 802.15.4, then we will never hear about IEEE 802.15.4; instead, we can hear about the products ZigBee, 6LowPAN, *etc*. Among all these technologies, the most popular one is ZigBee. IEEE 802.15.4 is a low-rate wireless personal area network (LR-WPAN). As the name indicates, it cannot be used for high-speed data transmission. It can be used with IoT devices. It makes use of a 2.4GHz frequency band, which is the same band used by Bluetooth and Wi-Fi. In this band, there are 80MHz available, so we can use sixteen 5 MHz channels out of it. We can get 250kbps out of that but we get only 50kbps upon the application. This limited data rate is due to the overhead at the wireless channel.

IEEE 802.15.4 makes use of the direct frequency spread spectrum technique for spreading the narrow band signal to a broad range of frequencies, and Carrier sense multiple access/collision avoidance (CSMA/CA) is used to minimize the collision when two or more stations send their signals over a data link layer. IEEE 802.15.4 is used for lower data rates, short distances, and lower energy utilization.

Mamatha Balachandra & Balachandra Muniyal

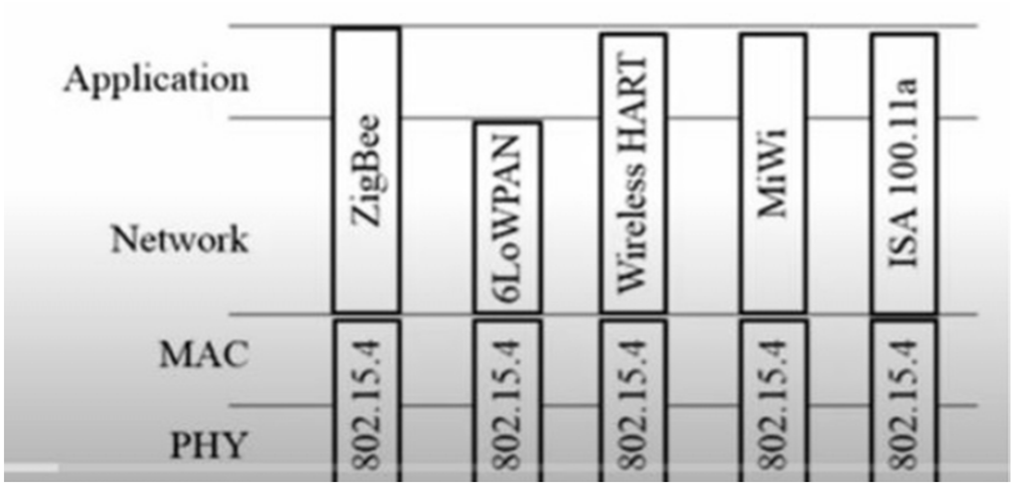

Fig. (1). WPAN standards.

Bluetooth (IEEE 802.15.4)

There are multiple ways to transmit data from one person to another . For example, data can be transmitted from one person to another either by sending it through WhatsApp or by emailing the data using the Internet. Rather than making use of the Internet to transmit data between the nodes, if we want to transmit data from one node to another wirelessly without the Internet, then both nodes should have Bluetooth adapters.

Bluetooth is a wireless technology standard used for exchanging information between fixed and mobile devices over a short distance using short wavelength Ultra High Frequency (UHF) radio waves in the ISM radio bands from 2.4GHz to 2.485 GHz, thus building Personal Area Networks. An industry consortium specifies Bluetooth called the Bluetooth Special Interest Group (SIG). This SIG specifies an entire suite of protocols that go beyond the link layer to define application protocols, which are called profiles for a range of applications. There exists a separate profile for separate applications. For example, we need a profile to synchronize PDA with personal computers or we may need a profile to give mobile computer access to a Wired LAN.

The basic Bluetooth configuration is called a Piconet. A sample Bluetooth Piconet is shown in Fig. (**2**):

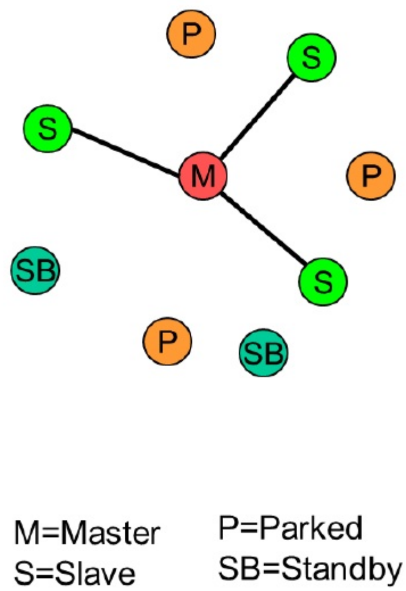

Fig. (2). Sample Bluetooth network.

In this network collection of devices is connected in an Ad hoc fashion. It contains only one master node, and other nodes are called slave nodes. Fig. (**1**) contains a Piconet having one master node and 8 slave nodes. Any communication in Piconet happens between the Master node and the Slave node. There is no direct communication possible between 2 Slave nodes. In case any two Slave nodes in the Piconet need to communicate, then communication should happen through the Master node only.

A slave node can also be set to an inactive state known as a parking state. Suppose a slave node is not at all participating in communication for a long time; then such a slave node state can be brought into a parking state to save the battery power. At a time, any number of slave nodes can be kept in a parking state. The parked slave nodes will be at inactive low power energy saving state. The collection of Piconets is known as scatternet. The sample scatternet is shown in Fig. (**3**).

This scatternet contains 3 different piconets. Every piconet contains a single master and several slave nodes.

Fig. (**4**) shows a set of Bluetooth adaptors that are used to frame the Bluetooth network. Bluetooth can connect fixed devices as well as mobile devices. We need to connect to a desktop computer using a Bluetooth adaptor to connect to some other device, maybe a mobile device, to establish short-range communication. We have many such adaptors with different connectivity requirements.

CHAPTER 6

Wireless Sensor Networks

Abstract: A Wireless Sensor Network (WSN) is a category Network. As the name suggests, the nodes are capable of sensing. Sensing is a physical phenomenon that occurs around them. Sensor nodes of WSN can sense humidity, pressure, temperature, light, sound, vibration, color, *etc*. Sensor nodes have one main component called a sensor, and these sensor nodes collectively make a network known as WSN. WSN is one of the very popular networks due to diverse types of applications, such as tracking objects, healthcare, agriculture, space applications, and so on. WSN is a key formation of the Internet of Things (IoT). IoT and WSN have been very important components for building smart cities in recent years in our country as well as across the globe. In this chapter, the need for WSN, the building block of WSN, the next design of WSN, the application of WSN, *etc*., are discussed.

Keywords: WSN, Sensors, WSN architecture, WSN applications.

INTRODUCTION

WSN is a collection of different sensors; these sensors are densely deployed and can capture the variety of physical phenomena occurring around them. Sensor nodes can be equipped with various types of sensors. Sensor nodes can collaborate and measure sound, light, temperature, *etc*., from surrounding environments. This sensed data can then be converted to digital signals and then processed to reveal the properties of the phenomenon.

Usually, sensor nodes are capable of capturing data from short distances through radio transmission range; however, by using relay nodes or intermediate nodes in WSN, it is possible to communicate nodes that exist from long distances. So, what we essentially see here is similar to what we observed in the case of an Ad doc network or multi-hop kind of architecture. Basically sensor network is used to sense data from short-range distances using a wireless medium, and by using multi-hop architecture, they transmit the data to the destination node, which is far apart. The destination node in WSN is termed a sink node or base station. There is a difference between the sink node and the base station. The sink node is necessarily a sensor node, whereas the base station may not be a sensor node. For example, there can be a computer at the sink node that will be stored in that computing device.

Mamatha Balachandra & Balachandra Muniyal

Why do we need a Sensor Network? What is the Difference between a Sensor and a WSN?

Individual sensor nodes embedded with sensors can sense the phenomena locally in a fixed location, whereas in WSN, it is possible to deploy multiple such sensor nodes over a large distance, which can even communicate with each other to get an idea about what is happening in such a larger area. So basically, to cover bigger areas, WSN becomes useful. WSN is also very useful when someone wants to observe or monitor such areas remotely in an unmanned fashion to find out what is happening in that larger area. Typical WSN is as shown below in Fig. (**1**).

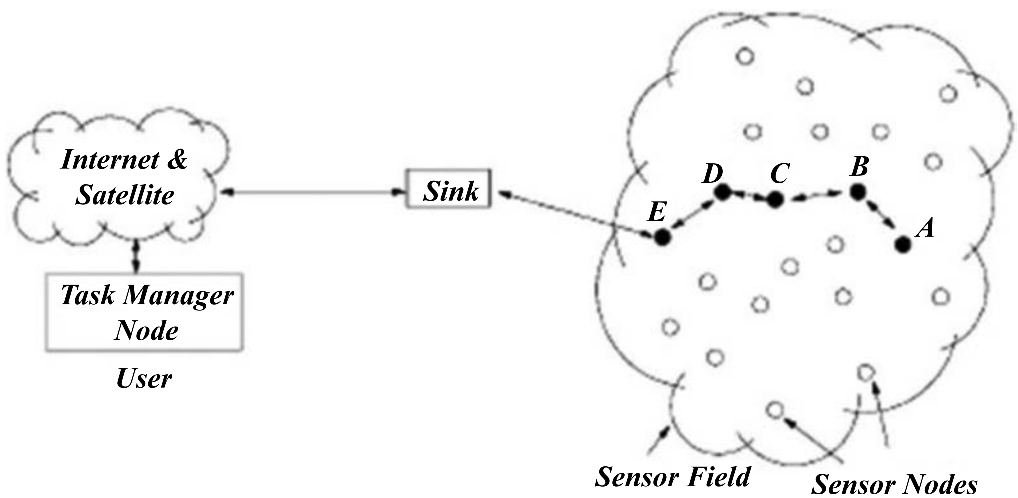

Fig. (1). Typical WSN.

Classification of WSN

WSN is broadly classified into two types: Stationary and Mobile.

a. **Stationary WSN:** This is a classical form of sensor network. In stationary WSNs, nodes in the network are fixed. None of the nodes is mobile.
b. **Mobile WSN:** In Mobile WSN, at least one or all the sensor nodes are mobile. Here, some of the nodes or all nodes would move. Mobile WSN is used in plenty of applications. This WSN is found mostly in oceans, terrestrial environments (Sensors fitted to vehicles), aerial sensor networks, or UAVs (Unmanned Aerial Vehicles).

Basic Architecture of WSN

A typical sensor node in WSN can communicate with each other through radio signals. Each sensor node in WSN is capable of sensing using its sensing unit, processing using its processing unit, and communicating using a transceiver unit. Sensor nodes in WSN have limited processing speed, limited storage capacity, and limited bandwidth. In addition to 4 units, application-dependent units are also present in WSN. This means whatever we have seen in a mini computer is available in sensor networks such as input units or sensing units, communication facilities, processing units, and output units. Fig. (**2**) shows the basic architecture of WSN.

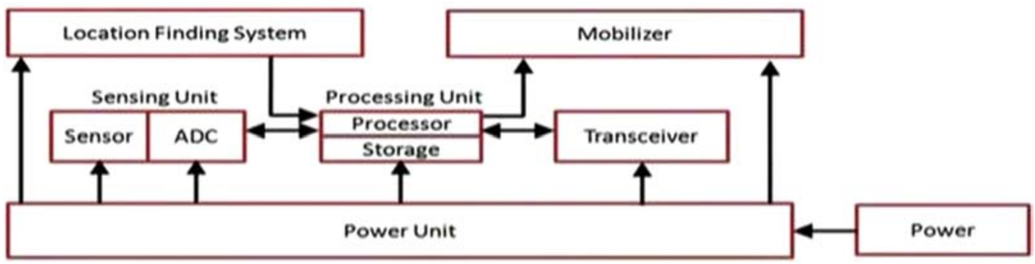

Fig. (2). Basic architecture of WSN.

Constraints on the Sensor Nodes in WSN

The following shows the constraints on typical sensor nodes in WSN:

a. *Be small in size:* Typically, less than a cubic centimeter.
b. *Consume less energy:* Nodes in WSN consume very low energy.
c. *Operate in an unattended manner:* Nodes in WSN are designed to operate in an unattended manner in a highly dense area.
d. *Low cost:* Sensor nodes are available at low production costs. Nodes can also be fabricated at low cost; hence, if the node is damaged for one or another reason or drains out of energy, then they can be dispensable.
e. *Be autonomous:* Sensor nodes, once deployed, operate autonomously in any area without human intervention.
f. *Be adaptive to the environment:* If there is a change in the environment, then nodes should be in a position to recognize that change accordingly.

Challenges to be Faced in Building Sensor Networks

For any typical application, WSN needs to be designed and implemented. Some of the common challenges to be faced in building a sensor network are listed below:

CHAPTER 7

Fundamentals of 5G Networks

Abstract: 5G is one of the emerging cellular networks, which is the successor of the 4G cellular network. Even though 5G technology development started in the year 2010, its deployment started in the year 2019. In 2020, 5G was deployed in a full-fledged manner. 5G supports several applications, such as enhanced broadband, smart cities, vehicle-to-vehicle connectivity, *etc*. It uses one of the new technologies, MIMO. 5G and IoT are powerful combinations for connectivity. 5G technology has marked a transformative era in the realm of connectivity, promising speed, low latency, and enhanced network capability. The proliferation of IoT devices on 5G presents security challenges, as many devices lack security features.

Keywords: 4G, 5G, IoT, LTE, Massive MIMO, MIMO, OFDM.

INTRODUCTION

Fifth-generation wireless communication is very different from its earlier generations. In the case of earlier generations, it was more about data rates and spectral efficiency, whereas in 5G, millions of technologies must come together in terms of various layers, from the physical layer to the access layer and the network layer. This generation was deployed in 2020, so 5G is also known as IMT 2020. In 2015, the International Telecommunication Union (ITU) established a focus group IMT. Its main task is to analyze how emerging 5G technology will interact with the future network. The main aim of ITU is to identify the KPI(Key Performance Identifier) requirements of the current generation. The study that was conducted covered high-level network architecture, end-to-end QoS framework, emerging network technologies, mobile front-haul and back-haul, and network softwarization. 5G gives all that is given by 4G. In addition to this, it gives something even better. 5G was deployed in almost all places of the world in 2020. This is the era of the Internet of Things [1, 2].

The requirement of 4G in terms of data rate was only up to 10Mbps, but for 5G, it is up to 100Mbps. The mobility of 4G (LTE advanced) is supposed to serve 350km per hour, and the requirement of 5G is 500km per hour, mainly for bullet trains. The latency requirement of 5G is 1 msec. Another important concern about

Mamatha Balachandra & Balachandra Muniyal

5G is that it must support 1 million devices per square kilometer. Here, the devices are nothing but IoT devices.

To meet the above requirements, ITU has made certain use cases. Some of the important use cases are enhanced broadband, scalability, tactile Internet, high-speed mobility, vehicle-to-vehicle communication, smart cities, rural connectivity automation, *etc*.

5G Internet

5 key characteristics of 5G, which make it better than 4G, are:

i. Better or optimized signals
ii. Efficient transmission
iii. Green signaling
iv. Low latency design
v. Larger bandwidth

Better Signals

The base station serves multiple users at the same time. For this, the spectrum has to be divided using OFDM. Here, OFDM is the advanced version of FDM. OFDM is the heart of 4G as well as 5G. The difference is that in 4G, the smallest division we can make in the spectrum is up to 15kHertz. But there is no such division in 5G; that is, we can have spectrum division of up to 120kHz. Not only that, we can mix and match. 5G waveforms are optimized much better than 4G. So, 5G OFDM is much more advanced than 4G.

Efficient Transmission

Green Signaling

Look at the KPI(Key Performance Indicator) based on the energy efficiency of the network. For efficient transmission, all the required KPIs are achieved in this type of network.

Low Latency Design

It is nothing but a faster response. Because of this, we can play online games, and we can implement control systems on a 5G network. This completely depends on how the signaling happens, and waveforms are transferred.

Larger Bandwidth

5G systems operate with a larger bandwidth than the 4G systems. For this, the requirement is to use the new set of frequencies, especially the millimeter range of frequencies. Because of this characteristic, it is possible to get a high range of throughput from the 5G networks.

5G Working

How does OFDM make 5G functional?

It serves multiple users so that they can operate with a reasonably high data rate. Given a base station and a bandwidth/spectrum, how can the base station serve or transmit data to multiple users? The basic idea here is to divide the spectrum into multiple smaller spectrums and use each of these spectrums to serve multiple users. Once these spectrums have been used for the list of users, then again provide the spectrum to another set of users. This is called FDM. OFDM is the smart way of achieving FDM. OFDM is the smart way of implementing the frequency division function. Fig. (**1**) shows the division of the frequency spectrum for multiple users:

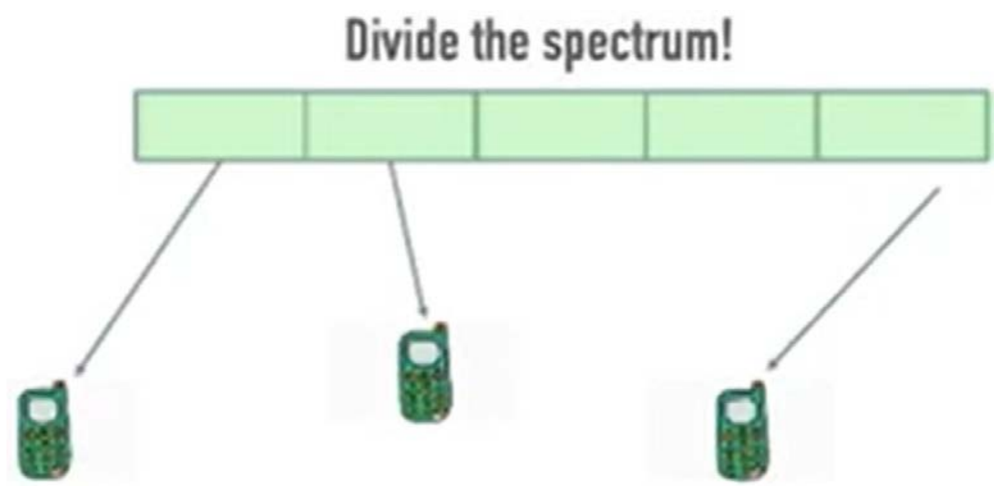

Fig. (1). Dividing frequency spectrum for multiple users using OFDM.

OFDM has been used earlier in 4G networks as well as Wi-Fi. OFDM is an advanced version of FDM. OFDM is the main core or heart of 4G as well as 5G. How does OFDM in 5G differ from 4G? In 4G, the smallest spectrum that we can make for each user is 15KHZ, whereas 5G provides multiple such options. With 5G OFDM, it is possible to make a frequency spectrum of variable sizes such as

CHAPTER 8

Internet of Things

Abstract: The Internet of Things (IoT) is a network comprising things or objects that are assigned unique identities and connected to the Internet. As per the statistics, by 2030, there will be approximately 30 billion devices or things connected to the internet [1]. These networks not only connect things to the Internet but also allow them to communicate and exchange information with each other. To establish connectivity between the various devices and the Internet, IoT uses important protocols such as MQTT, 6LowPAN, Bluetooth, RFID, ZigBee, CoAP, *etc*. IoT is useful in all types of applications, such as healthcare monitoring, agricultural domains, mining, and space applications. IoT real-life application generates a large volume of data, which is analogous to Big Data, which needs to be processed, stored, and analyzed to extract useful information. IoT is shaping the way we live our lives.

Keywords: Bluetooth, CoAP, Gateway, IoT connectivity, IoT WAN, IoT LAN, MQTT, 6LowPAN, RFID, ZigBee.

INTRODUCTION

IoT, as the name suggests, starts with the word ‘Internet’, which is nothing but a connection of computers as well as computer-oriented devices. The Internet is a global network. Nowadays, the Internet of Things is one of the hottest technologies across the globe. All types of organizations, government or private, and industries are involved in different aspects, such as implementation, business, and research on IoT. Currently, a lot of investments are being made in almost all these organizations for the development of the Internet of Things.

Nowadays, the Internet of Things is becoming more popular in all types of applications, such as healthcare monitoring, agricultural domains, mining, and space applications. Across the world, there has been a lot of interest in developing smart city applications such as smart surveillance to detect if any illegal activity is going on. Next is the smart health application, wherein the patient is allowed to check which hospital provides which type of facility and accordingly makes use of it without physically moving to the required location to get the required information. Similarly, smart parking is another application of IoT, wherein people easily identify free slots and park their vehicles over there, especially

Mamatha Balachandra & Balachandra Muniyal

during peak hours; otherwise, it is very difficult to identify free parking locations. Next is smart home applications, which may be related to household resource monitoring or taking care of elderly people who are staying alone. Using IoT, it is possible to control or monitor the working of essential household appliances from remote places, and it is even possible to watch remotely whether elderly people are facing any problems at home or not.

IoT is one of the very popular evergreen technologies that make our lives very simple and also enhance the quality of life without much investment. Using IoT, we can connect all of our appliances to the Internet and monitor them remotely. Because of IoT, we can build several multidisciplinary applications in our day-to-day lives.

Equation of IoT

IoT= Physical object +

Controller, Sensor, Actuator +

Internet

IoT is nothing but a connection of computers and computer-oriented devices. The Internet is a global network. Now comes the point: 'Why is IoT needed?'. Very soon, most of the things that we see around us will get interconnected.

Devices used in IoT are categorized into two groups: Basic Devices and Advanced Devices.

i. Basic Devices: These are devices that only provide the fundamental services to an application, such as sensing useful data or actuating tasks with limited human intervention. These devices are connected to local networks *via* technologies such as ZigBee, Bluetooth, Wi-Fi, cellular networks, *etc*.
ii. Advanced Devices: The large volume of data that is collected through sensors from various distances for an application requires to be processed to get useful information out of it. Data may also have to be ported to the cloud through a WAN connection. The types of devices that fall under this category are Gateway devices and Cloud Platform.

Deployment can differ for basic and advanced deployment scenarios. Deployment scenarios for basic devices include smart gardening, smart home monitoring, *etc*. In such applications, sensors such as temperature sensors, soil moisture sensors, and humidity sensors are involved, and the central unit takes care of application logic. The central unit can also be connected to WAN.

Deployment scenarios for advanced devices include smart meters. In such applications, meters are installed in houses or organizations for measuring electricity, gas, water, *etc*. Here, the central gateway collects data from the meters from various household and organization premises and then aggregates the data. Finally, the data is sent to either server through a cellular connection for generating the invoices.

Implementation Aspects of IoT

To implement IoT, we need to understand the fundamental basics behind IoT, the basic technology, network connectivity, and the devices required to establish the connection. The Internet is a global network in which different computers are interconnected. IoT is beyond this technology, wherein various things or physical objects that we see around us get interconnected. The things may be fans, lighting systems in a room, refrigerators, and anything in a room, including a microwave oven, television, and so on. Internetworking of devices is not only limited to homes and industries but also extends to various business activities. Now, the question is why this IoT has become so popular? The reason is that IoT provides an advanced level of services to society, businesses, and so on. Numerous IoT-related devices that we use in our daily lives rely on embedded systems, embedded electronics, embedded communication systems, *etc*., so that they make use of some common platforms. Each thing under this network is treated as a node. The outcome of connecting this device is a very large network, which is larger than the normal Internet.

IoT is now used widely in smart homes and smart city applications not only in India but also in the entire globe. In IoT, nodes are interconnected using wireless technologies. As of now, over 9 billion devices are interconnected in IoT networks. Soon, this count may go beyond 20 billion. So, in the near future, billions or trillions of things are going to be interconnected.

There are two different approaches in which IoT can be built. The first one is connecting things to the existing network, and the second approach is to build the network from scratch. Each approach used in building the IoT has its challenges that have to be taken care. In IoT, there can be a variety of devices with different configurations. The unification of all these devices is very much required as IoT is not a single technology. Each of the things in the IoT may be of different configurations, different specifications, and so on. Each of them may be supported by many other technologies, such as cloud computing, big data, machine learning, computer vision, *etc*. So, developing IoT solutions requires expertise from various disciplines, such as computer science, electrical engineering, and mechanical engineering.

CHAPTER 9

Fundamentals of 6G Networks

Abstract: 6G is the successor of the 5G cellular network. It is one of the ongoing research areas whose deployment started recently. It makes use of different potential technologies and Terahertz communication. There are a lot of research opportunities in 6G as it is still in the implementation stage. The architecture of 6G is wider. This means the architecture of Terahertz communication covers space, air, ground, and underwater networks, and all segments of the communication network come together and work under the same umbrella, framing ubiquitous connectivity. Potential 6G technology includes 6G with full integration of AI with big data analytics, novel radio access technology, Super Massive MIMO, and quantum computing. The targetted full-fledged deployment of 6G is expected or ITM (International Mobile Telecommunication) by 2030.

Keywords: 6G, 5G, 4G, Super massive MIMO, Terahertz communication.

INTRODUCTION

With this upcoming wireless network, several ambitious key possibilities of 6G exist for the users. They are as follows:

i. The peak data rate that is targeted for 6G is in Terabytes, which is approximately 100 times that of 5G. So there is a tremendous increase in data rate of 6G. The requirement of one user's data rate is approximately 1GB, which is 10 times greater than that of 5G wireless networks.
ii. The range of frequency targeted for 6G is 0.1 to 10 THz (Terahertz). As the frequency targeted in 6G is very high, several challenges need to be addressed due to this.
iii. The spectrum efficiency of 6G is 5 to 10 times as much as that of 5G.
iv. Operates at very high mobility.
v. Latency could be very low: Whenever there is high mobility in the wireless network, the latency could be very low, which is in the order of 10 to 100 microseconds.
vi. The connectivity density of 6G could be at least 10 times the connectivity density of 5G.

Mamatha Balachandra & Balachandra Muniyal

vii. Energy efficiency is also required to be at least 10 times higher than that of 5G technology.
viii. Substantially high throughput.
ix. Enhanced data security.
x. Ubiquitous connectivity: Ubiquitous connectivity is needed in 6G to support AI-integrated communication.

Comparison of 6G with 4G and 5G

Table **1** shows the comparison of 6G with 5G and 4G in terms of data rate, AI support, extended reality, satellite communications, and so forth:

Table 1. Comparison of 6G with 4G and 5G wireless networks.

Type of Network	THz Communication	Haptic Communication	AI Integrated	Extended Reality	Satellite Communication
4G	Does not support Terahertz communication; instead, it supports from 2.4GHz to 5 GHz	Does not support Haptic Communication	Integration of Machine Learning and Deep Learning is not there	Does not support extended reality	Does not support Satellite communication
5G	Marginal support for Terahertz communication, *i.e.*, from 28 GHz to 30 GHz	Marginal Support for Haptic Communication	Marginal support for AI is provided	Marginal support for extended reality	Does not support Satellite communication
6G	Supports substantially high frequency for THz communication from 0.1 THz to 10THz.	Substantial support for Haptic Communication	Targeted with complete implementation of AI	Full-fledged support is provided for extended reality	Support Satellite communication

6G ELECTROMAGNETIC SPECTRUM

For 4G LTE, around 6GHz of frequency is supported whereas, for 5G networks, the targeted frequency is around 30GHz. However, for 6G, what we can expect is beyond 100 GHz of frequency to 10 THz. It is very difficult to design the hardware components that utilize high frequency as it may damage the system. So initially, people targeted designing equipment that utilized less frequency of 6G spectrum, *i.e.*, around 100 GHz to 300 GHz. Later, based on the requirements, they started increasing the frequency range, for example, from 300 GHz to 3 THz. As per the literature, it is found that generally, this frequency range is not as harmful as Xray and Gamma-ray frequencies, which have a frequency of 10^{15} to

10^{18}, respectively, which can damage the human body cells. So, the frequency range of up to 3 THz is still under study as to whether Terahertz communication can damage human body cells. One of the advantages of Terahertz communication is that we can achieve throughput. Some of the important features of 6G are discussed below:

i. With the Terahertz frequency range, there will be more bandwidth, so we can achieve very high data rates. *i.e*., the data rate will be in terms of Terabits per second.
ii. There could be a chance of high path loss rising from high frequency. Due to this problem, it is not possible to transmit signals over longer distances. This could be one of the disadvantages of Terahertz frequency. So, 6G can transmit over shorter distances compared to 4G and 5G. Wider coverage is a challenge. This disadvantage can be overcome by using more towers with beam-forming antennas to encompass the path losses.

6G CHALLENGES

i. **Atmospheric attenuation or atmospheric absorption:** As the frequency increases, the overall attenuation also increases. This means that for lower frequencies, such as 6 GHz to 120 GHz, the atmospheric attenuation is not that high, whereas for frequency above 100 GHz, the attenuation increases rapidly, as shown in Fig. (**1**). This increase in attenuation will deteriorate or degrade our signal. So this means that we not be able to receive the signal with a higher signal-to-noise ratio. This will degrade the Quality of Service.
ii. **Surface scattering:** Most of the lower frequency signals appear smoothly on most of the surfaces. There can be minor scattering but not much trouble with lower frequency, whereas, with the Terahertz spectrum, there is significant diffuse scattering and strong specular reflections. So this can be a major trouble that can degrade our signal quality.
iii. **Partition and penetration losses:** Partition and penetration losses are substantially high as the frequency increases. The higher the frequency, the higher the attenuation in 6G. Also, it depends on the thickness of the material used. The larger the thickness, the larger the attenuation. For example, if we consider a glass or glass wall, we will see an attenuation of 15 to 28 DB (Decibel) based on what frequency we employ and the thickness of the material. If we take wooden material with 0.25 to 0.75 thickness and at Terahertz frequency, we will observe around 14 to 26 DB attenuation. Similarly, for plastic and paper, we will see very large attenuation at higher frequencies. This will directly impact the signal to noise ratio as the higher the path, the higher the penetration loss. So, we will not be able to deliver a signal

SUBJECT INDEX

A

Ad hoc network 1, 43, 45, 46, 49, 54, 55, 60, 65, 66
Ad Hoc on-demand distance vector routing 63
Advanced mobile phone system (AMPS) 21, 22, 23, 24, 42
Airdrop feature 73
Algorithm 28, 41, 56, 66
  complicated 56
Amplitude 9
  modulation 9
  modulation technique 9
AMPS 22, 24
  channels 22, 24
  network 22
Analog 9, 21
  mobile telephone system (AMTS) 21
  modulation techniques 9
Android smartphones 119
AODV route discovery 64
Apple devices 73
Application(s) 5, 17, 29, 65, 67, 72, 74, 75, 77, 81, 82, 87, 88, 101, 102, 108, 110, 118
  connectivity 17
  industrial 74
  landslide 75
  multidisciplinary 102
  support sublayer (ASS) 108
Applications of WSN 75, 78, 85, 88
  in healthcare 85
  in precision agriculture 88
Architecture of terahertz communication 127, 130
Arduino IDE android smartphone 119
Artificial Intelligence 131
Atmospheric absorption 129
Attenuation, atmospheric 129
AUC Authentication center 27
  and subscriber key 27
  authenticates mobile subscribers 27
Automated electronic triage telemedicine system 87
Automatic teller machines 104

B

Bandwidth 11, 13, 14, 18, 20, 21, 23, 35, 37, 38, 40, 43, 56, 97
  for wireless access based on geographic location 40
  ranging 40
  wastage 11
Beam theorem 97
Big data analytics 131
Bits 18, 22, 29, 40, 41, 51, 111, 131, 132
  digital 41
  guard 29
  synchronization 18
  traditional 132
  training sequence 29
Bluetooth 67, 68, 69, 70, 71, 72, 73, 75, 77, 101, 102, 105, 106, 114, 115, 119
  adapters 68
  and transferring files 73
  applications 72, 114
  communication 71
  connections 115
  devices 70, 71, 115
  low energy (BLE) 105, 119
  network 69
  security 72, 115
  technologies 72, 75, 114
  wireless connection 115
BPSK and QPSK modulation techniques 75
Broadband wireless access (BWA) 50
Building sensor networks 80
Business activities 103

C

CDMA 18, 31, 33
  applications 33

Mamatha Balachandra & Balachandra Muniyal

network technologies 31
signal 33
technique 18
Cellular 11, 14, 16, 18, 20, 21, 23, 24, 35, 37, 42, 92, 98, 132
architecture 18
networks, emerging 92
systems 11, 14, 16, 21, 23, 24, 35, 42, 98, 132
technology 20, 37
wireless networks 20
Circuit, integrated 113
Circuitry, small integrated 113
Cloud 102, 103, 122
computing 103, 122
Code(s) 11, 13, 14, 18, 20, 31, 32, 33, 34
division multiple-access (CDMA) 11, 13, 14, 18, 20, 31, 32, 33, 34
pseudorandom 33
Coding techniques 47
Collision 48, 58
detection 48
problems 58
Commercial building automation 74
Communication 118, 119, 123, 127, 130
devices 119
network 127, 130
technologies 118, 123
Comparison of traditional wired networks 43, 51
Computer(s) 1, 2, 5, 72, 78, 103
vision 103
Computing 1, 78, 127, 132
device 1, 78
quantum 127, 132
Connect IoT devices 18
Connection 1, 2, 17, 20, 52, 71, 72, 98, 103, 104, 114, 115
cellular 103
radio frequency 1, 20
wired 1, 2, 114
Connectivity 5, 17, 82, 83, 92, 93, 98, 101, 104, 105, 106, 116, 111, 114, 116, 124
automation, rural 93
framing 104
global unique 111
smart 116
vehicle-to-vehicle 92
wired PAN 114
wireless inter-network 17
Consumer electronics 98
Cordless telephones (CT) 3
Core network (CN) 27, 35, 37
Crop(s) 77, 88, 123, 124
insurance 123
organic 124

D

Data 7, 13, 29, 36, 63, 81, 121, 122
processing time 121
transmission 7, 13, 29, 63, 81
transport 36
transportation 122
Deployment 37, 51
cost 37
of fixed wireless networks 51
Destination sequence distance vector (DSDV) 54, 59, 60, 61, 62
Detection 23, 75, 85, 104
air pollution 104
applications 75
techniques 23
Devices 2, 30, 38, 51, 69, 72, 73, 86, 93, 97, 98, 101, 102, 103, 104, 110, 116, 118, 119, 122
biomedical 122
computer-oriented 101, 102
electronic 30
heart monitoring 116
Digital 3, 11, 23, 24, 32
advanced mobile phone system (DAMPS) 23, 24
arms 3
modulation 11
technology 23
wireless data transmission system 32
Direct spread spectrum (DSS) 73
Dynamic 35, 55
network topology 55
radio resource management 35
topology 55

E

Electromagnetic 5, 6, 8, 128, 132
spectrum 5, 6, 128, 132
waves 5, 6, 8
Electronic serial number (ESN) 22
Environmental factors 88

Equipment identity register (EIR) 27

F

Facial recognition 104
Fast fourier transform 41
Fixed 27
  line analog telephone systems 27
  telephones 27
Fleet management 29
Framing mesh topology 108
Frequency 7, 9
  modulation technique 9
  spectrum for data transmission 7
Frequency division 11, 13, 18, 23, 28, 32, 46, 94
  function 94
  multiple access (FDMA) 11, 13, 18, 23, 28, 32, 46

G

GFSK Gaussian Frequency Shift Keying modulation technique 75
Global special mobile 24
Green signaling 93
GSM 3, 8, 11, 24, 25, 28, 29, 30, 31, 32, 35, 36, 42
  and CDMA network technologies 31
  architecture 25
  mobile phone 8
  network architecture 25
  technologies 35

H

Haptic communication 128
Hardware platforms 118
Healthcare industry 116
High-speed 38, 98
  applications 38
  data transfer 98
Higher frequency bands 37
Hop reservation multiple access (HRMA) 57
Horizontal zoom technologies 121
Human-computer interactions 131
Hybrid routing protocols 60

I

IMT International Mobile Telecommunications traffic 116
Industry automation 1
Infrastructure 46, 49, 52, 65, 66, 98, 99, 116, 118, 122, 123
  cloud 118
  global 123
  intelligent 98
  WLAN 46
Installation 43, 45, 49, 51
  flexibility 45
  of wireless LANs 45
Integrated customer services 4
Integration 17, 19, 90, 98, 105, 123, 124, 127, 128, 131
  of machine learning and deep learning 128
  of wireless networks 17
Intelligent transportation 65
Inventory control system 83
Inverse fast fourier transform 41
IoT 19, 98, 101, 106, 107, 116, 123, 124
  application of 101, 116, 123
  architecture 124
  for home automation 19
  gateway WAN 106
  industrial 106, 107
  integration 98
IoT connectivity 101, 105, 117, 124
  technology 117
  Terminology 105
IoT device(s) 92, 99, 119
  deployment 119
  proliferation of 92, 99

K

Key performance indicator 93

L

LAN technology 44
Licensed technology 20
LLC layers 108
Logical link control (LLC) 44, 71, 107, 114
  adaptation protocol (LLCAP) 71
  layer 44
Long-distance radio communication 7
Low 80, 93, 107

latency design 93
power consumption applications 107
production costs 80

M

MAC protocol 55, 56
Machine(s) 88, 103, 105, 107, 128
industrial 107
learning 88, 103, 128
MANET(s) 55
challenges 55
dynamic topology 55
Massive MIMO technology 99
Microwave access 37, 50
MIMO techniques 96
Mobile 8, 21, 24, 27, 28, 31, 54, 56, 59, 60, 68, 69, 79, 82, 114, 116, 119, 132
communications 24, 27, 31
computer communication 8
devices 68, 69, 114, 116
sensors 82
telephone system 21
Modulation techniques 8, 9, 18, 71
Monitoring 30, 75, 77, 84, 99, 102, 104, 107, 110, 130
agricultural 75
animal 75
earthquake 104
remote 130
smart home 102, 110
Multiple 4, 56, 57, 56, 92, 95, 132
access with collision avoidance (MACA) 56, 57
access with collision avoidance for wireless (MACAW) 56
input, multiple output (MIMO) 4, 92, 95, 132
output systems 4
Multiplexing techniques 40

N

National institute of standard technology (NIST) 121
Networks 38, 36, 104, 130
switched 38
terrestrial 130
traditional 104
transmission 36
NoSQL database systems 123
Novel radio access technology 131

O

OFDM 40, 41, 47
techniques 40, 47
transmitter maps 41
Optical 131
fiber cable communications 131
wireless communications 131
Orthogonal 40, 41
frequency division multiplexing 40
multicarrier techniques 41

P

Packet binary convolution coding (PBCC) 47
PAN topology 111
Point coordination function (PCF) 48, 49
Public switched telephone networks (PSTN) 15, 27

R

Radio 7, 17, 36, 43, 72, 114, 115
frontend component (RFCOMM) 72, 114, 115
network controller (RNC) 36
network system 36
technology 17
transmissions 7, 43
Radio frequency (RF) 1, 7, 20, 21, 51, 55, 104, 112, 115
bands 55
Reverse voice channel (RVC) 22, 24
RFID tags and sensor networks 118
Roadside access point (RSAPs) 65
Routing 4, 55, 58, 59, 60, 61, 62, 63, 66, 75, 111, 112
mesh-based 111
process 60
protocols 59, 60, 61, 62, 111
reactive 60, 62, 63, 112
RPL Protocol 112
IPv6 Routing protocol 112

S

Second-generation GSM technology 3
Secret message transmission 33
Security 5, 23, 27, 51, 55, 71, 75, 76, 81, 99, 108, 110, 114, 116, 118
  issues 51, 99
  policy 108
  threats 55
Sensing 49, 78, 80, 83, 88, 123, 130, 132
  nodes sense 88
Sensor(s) 75, 76, 78, 79, 81, 82, 83, 84, 85, 86, 87, 88, 102, 104, 118, 119, 120, 123
  based irrigation system 75
  camera 120
  humidity 102
  network protocol stack 76
  single 85
  soil moisture 102
Sensor networks 76, 78, 79, 80, 81, 82, 104, 112, 118
  deployment 81
  wireless image 76
Service(s) 2, 3, 21, 29, 30, 37, 65, 71, 72, 98, 103, 107, 108, 115, 118, 121, 122
  broadband 37
  connection-less 115
  discovery 71
  industry 30
  mobile telephone traffic 21
  real-time 121
  restoring fundamental resource 118
  specific convergence sublayer (SSCS) 107, 108
  telephonic 72
Signal 9, 29, 32, 45, 78, 95, 97
  amplitude-modulated 9
  audio 9
  broadband 32
  digital 78
  frequency-modulated 9
  infrared 45
  narrowband 32
  propagation 97
  transmission 29, 95
  wideband 32
Smart 101, 102, 103, 131
  city applications 103
  health application 101
  home applications 102, 131
Soil 75, 77, 88
  humidity 77
  moisture levels 75, 77
Spectrum technique 67

T

Techniques, soft computing 88
Technologies, data-handling 122
THz communication 128
Time division 11, 12, 32, 35
  duplexing (TDD) 12, 35
  multiple access 11, 32
Topological information 60, 61
Transmission, efficient 93
Transmit signals 129
Transmitting data 108

U

UMTS radio access network (UTRAN) 35, 36

V

Value-added service (VAS) 30
Vehicle-to-vehicle 93, 97
  communication 93
  technology 97
Vehicular 54, 65, 66
  Ad hoc networks (VANETs) 54, 65, 66
  communication system 54
Visible light communication (VLC) 132

W

WAN connection 102
Wi-Fi 18, 51, 52
  chips 18
  hotspots 51
  routers 52
  signal 52
  technology 18
Wired 6, 51
  networks wireless networks 51
  transmission 6
Wireless 3, 4, 5, 6, 14, 17, 18, 20, 26, 43, 46, 50, 52, 54, 59, 60, 62, 67, 72, 74, 76, 77, 82, 103, 123
  Ad hoc network 54

application protocol (WAP) 72
camera system 74
communication 4, 5, 18, 26, 50
image sensor network (WISN) 67, 76, 77
LAN technology 46, 52
local area network 17, 20, 43
networking 46
networks, digital 14
routing protocol (WRP) 54, 59, 60, 62
sensors 82, 123
technologies 3, 103
transmission 6
wide area network 20
Wireless broadband 37, 43
services 43
systems 37
WLAN technology 43

Z

ZigBee 108, 110
device object (ZDO) 108
end device (ZED) 110
router (ZR) 110

Mamatha Balachandra

Dr. Mamatha Balachandra is currently working as a Professor in School of Computer Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. She obtained her B.Tech in Computer Science and Engineering from Mangalore University, and her M.Tech and Ph.D. in Computer Science and Engineering from the Manipal Academy of Higher Education, Manipal.

Her research areas include Mobile Ad Hoc Networks, IoT in Agriculture, IoT & Blockchain Technology, and Network Security. She has around 28 years of teaching experience and has published more than 50 research papers in national and international journals and conferences.

She is currently guiding eight Ph.D. students under the Manipal Academy of Higher Education. She also serves on the editorial board of several journals and has been appointed as the Governing Board Member for the International Cyber Security Data-mining Society (ICSDS) representing India.

Balachandra Muniyal

Dr. Balachandra received his B.E. degree in Computer Science and Engineering from Mysore University, India, and his M.Tech and Ph.D. in Computer Science and Engineering from the Manipal Academy of Higher Education, Manipal, India. He completed his M.Tech project work at T-Systems Nova GmbH, Bremen, Germany. His research area is Cyber Security. He has more than 90 publications in national and international conferences and journals.

Currently, he is working as a Professor in School of Computer Engineering, Manipal Institute of Technology, Manipal. He served as Head of the Department from 2017 to 2020. He has 30 years of teaching experience in various institutes. He was deputed to Manipal International University, Malaysia, from January 2014 to January 2015.

Under his supervision, eight research students have completed their Ph.D., and he is currently guiding eight more research students.