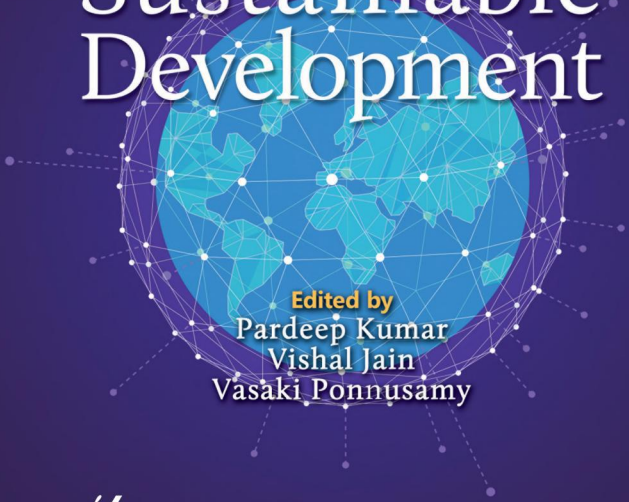
The Smart Cyber Ecosystem for Sustainable Development



Edited by
Pardeep Kumar
Vishal Jain
Vasaki Ponnusamy

Scrivener Publishing

WILEY

The Smart Cyber Ecosystem

This edition first published 2021 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-119-76164-8

Cover image: Pixabay.Com
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The cyber ecosystem consists of a huge number of different entities that work and interact with each other in a highly diversified manner. In this era, when the world is surrounded by many unseen challenges and when its population is increasing and resources are decreasing, scientists, researchers, academicians, industrialists, government agencies and other stakeholders are looking forward to smart and intelligent cyber systems that can guarantee sustainable development for a better and healthier ecosystem. The main actors of this cyber ecosystem include the Internet of Things (IoT), artificial intelligence (AI), and the mechanisms providing cybersecurity.

This book attempts to collect and publish innovative ideas, emerging trends, implementation experiences, and pertinent use cases for the purpose of serving mankind and societies with sustainable societal development. As outlined in the Table of Contents, the 22 chapters of the book are divided into three parts: Part I deals with the Internet of Things, Part II focuses on artificial intelligence and especially its applications in healthcare, whereas Part III investigates the different cybersecurity mechanisms.

In conclusion, we would like to express our great appreciation to all of those with whom we had the pleasure of working with during this project. First, the editors would like to express their deep and sincere gratitude to all the authors who shared their ideas, expertise, and experience and submitted their chapters in a timely manner. Next, the editors wish to acknowledge the extraordinary contributions of the reviewers for their valuable and constructive recommendations that improved the quality, coherence, and content presentation of the chapters. Finally, our heartfelt gratitude goes to our family members and friends for their love, prayers, and concern, allowing us to complete this project on time.

Dr. Pardeep Kumar
Dr. Vishal Jain
Dr. Vasaki Ponnusamy
July 2021

Part 1

INTERNET OF THINGS

1

Voyage of Internet of Things in the Ocean of Technology

Tejaskumar R. Ghadiyali[1]*, Bharat C. Patel[2] and Manish M. Kayasth[1]

[1]Udhna Citizen Commerce College & SPB College of Business Administration & SDHG College of BCA & IT, Surat, Gujarat, India
[2]Smt. Tanuben and Dr. Manubhai Trivedi College of Information Science, Surat, Gujarat, India

Abstract
In this technological era, the voyage of the Internet of Things (IoT) in the ocean of technology is very interesting, innovative, and beneficial to society. In this voyage, we have to deal with many icebergs in the form of technology such as Machine-to-Machine Communications, Cloud Computing, Machine Learning, Big Data, Distributed Systems, Smart Device, and Security. Blending of such technology with the IoT ultimately promises not only intelligent systems talking to each other but also with human beings in real time in varied domains such as Healthcare, Agriculture, Transport, Corporation services, Manufacturing, and other "Smarter" domains. In this chapter, during the voyage of IoT, we will elaborate Introduction (Basics of IoT, Characteristics, Base Architecture of IoT, and Merits and Demerits), Technological Evolution Toward IoT, Associate Technology in IoT, Interoperability in IoT, Introduction to Programming technology associated with IoT and IoT applications, and A special case study with "Smart Farming: A paradigm shift toward sustainable agriculture" which concludes the chapter.

***Keywords*:** IoT, Internet of Things, Associate Technology with IoT, Interoperability in IoT, Programming in IoT, IoT application, IoT in Agriculture, Smart Farming

1.1 Introduction

There are several motivated factors that tell us why the voyage of IoT is important in the ocean of technology. Current internet service basically provides a connection of computers and computing devices, whereas the Internet of Things (IoT) has expanded its scope from computers and computing devices to other things around us. IoT interconnects physical objects around us such as at home it can be communicated with lights, fans, air conditioners, refrigerators, microwave ovens, and other Bluetooth-operated devices, and at the workplace, it can be communicated with internet operated machines. In the recent era,

**Corresponding author*: tejas_ghadiyali@rediffmail.com

Pardeep Kumar, Vishal Jain and Vasaki Ponnusamy (eds.) The Smart Cyber Ecosystem for Sustainable Development, (3–24) © 2021 Scrivener Publishing LLC

such "Things" connected to the internet have crossed over twenty billion. Such things using embedded electronics are going to connect other things around them depending on the application requirements and thus construct a much bigger Inter-network of Things than that of the current internet of computers and computing devices called the Internet of Things (IoT). To do so, IoT devices have to deal with a challenge of interoperability, that means how such different objects can perform inter-communication with each other. So, this is the integral visualization of the IoT.

The other motivated factor in IoT technology implementation is of its low-cost IoT hardware. In IoT, connection of low-cost sensors with cloud platforms gives revolutionary results in this technological era. Using a legitimate merger of these technologies, we can track, analyze, and respond to operational data at a large scale. So, this feature leads toward the end of legacy closed, static, and bounded systems technology and creates a new paradigm of omnipresent connectivity. Such omnipresent connectivity enables communication and exchanges useful information between and with everyday objects around us in order to improve quality of human life. When objects can sense the environment and communicate, they become powerful tools for understanding complexity within it. Such smart objects that can interact with human beings are likely to be interacting more with each other automatically (without human intervention) and updating themselves their daily schedules [1].

Such a phenomenon in the 2000s was heading into a new era of ubiquity, the fact of appearing everywhere internet connectivity is not only serving for Anywhere, Anytime but it also gives the surface of connecting Anything. So, this concept will remove a separation between the real world (physical world) and an imaginary world (internet) resulting that real-world interest should be able to get access to online. In this online access, human beings are very less as internet traffic generators and receivers compared to the things (devices) around us. So, as per the Gartner Research, we can define IoT as, "*The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment*" [30].

1.1.1 Characteristics of IoT

The applicability and scope of IoT depends on its basic characteristics as given below [2].

Connectivity: Permits network accessibility and compatibility. Compatibility provides the ability to consume and produce data from the network while accessibility is the ability to avail network access.

Interconnectivity: This characteristic of IoT says that Anything around us can be Interconnected and thereby communicated with others.

Heterogeneity: The devices that are used in IoT are different in nature, hardware platform, and other network-related capabilities. Such devices are known as heterogeneous devices that can work together with each other in various networks.

Scalability: In IoT, the amount of devices connected with each other to perform communication is very large, i.e., in millions or even in trillions compared to existing internet. So, in this scenario, it is critical to manage and interpret the generated data that ultimately requires scalable data handling techniques. So,

even when internally connected devices such as sensors and other connecting devices increase, it should not affect network performance.

Dynamic: The devices connected with each other in IoT are changing not only their status from connected to disconnected, sleep to wake up but they also update their location as well as speed. Thus, it dynamically updates the number of connected devices.

Safety: As we have discussed, millions and trillions of devices are connected in IoT, so safety for data generators and data recipients is must. Such safety design should be made available to data in network, network endpoints, and network itself with sufficient scaling.

Having such characteristics, IoT architecture can be classified into three different tiers such as Physical Layer, Network Layer, and Application Layer as follows.

1.1.2 IoT Architecture

Different architectures have been proposed by different researchers for IoT, out of which the most popular architecture is three-layer architecture as shown in Figure 1.1. As per its name, this architecture has three layers, namely, i) Perception Layer, ii) Network Layer, and iii) Application Layer. This architecture basically provides the basic idea of the IoT that is further divided into five-layer architecture [2, 5, 20].

The Perception Layer is also known as a physical layer that consists of sensors and actuators. Sensors sense information from the surrounding environment and actuators actuate, i.e., perform some actions based on its sensing from the environment. So, actuators are mechanisms that control the system and accordingly act in the environment. So, basically, this layer provides/acts as input to the IoT architecture.

The Network Layer acts as an intermediate layer that provides communication between perception layer and network layer using communication devices such as routers and gateways. The basic task of this layer is to connect smart devices and its related servers. As an intermediary layer, it also transmits and processes the input data of sensing devices received from the perception layer.

The Application Layer defines various applications in which IoT is deployed. This layer performs application specific tasks and delivers service accordingly. The specific application may be smart farms, smart homes, smart cities, etc.

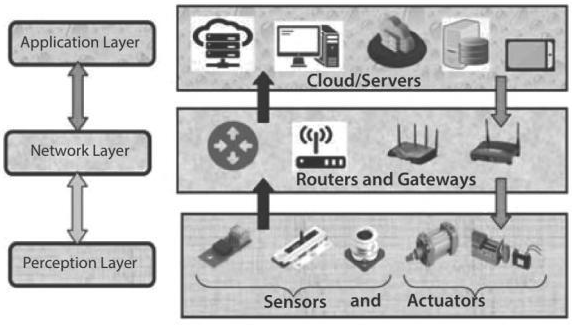


Figure 1.1 Three-layer IoT architecture.

Furthermore, this three-layer architecture converts into five-layer architecture. In this architecture, the perception layer and application remains and acts the same but the intermediate network layer is again divided into three sub layers such as Transport Layer, Processing Layer, and Business Layer. In this five-layer architecture, the transport layer transmits sensor data from perception layer to processing layer. Processing layer acts as a middleware layer and it can store, analyze, and process data that was received from the transport layer. To do such a task on data, this layer basically deals with many other data management technologies such as Big Data computing to process, cloud computing to store, and database management system to manage the data. The Business Layer acts on the top of the application layer and manages the entire IoT system. It consists of all application-related information such as profit model of business to that application, user privacy to the specific application, and other such business application-related information. Based on this architecture, the merits and demerits of IoT are as follows.

1.1.3 Merits and Demerits of IoT

Merits and Demerits of the IoT are as mentioned below:

Merits:

- ✓ Access Information: Due to association of cloud computing technology with IoT, the data access of the IoT is easy and available anywhere, anytime. So, a person involved in IoT can have easy access to such information and thereby without having his/her physical presence, it makes it convenient for that person to go about their work.
- ✓ Communication: IoT has important characteristics such as Interoperability. Using such characteristics, devices involved in IoT can easily talk to each other. In this way, inter-device communication will be more transparent and thereby increase efficiency of connected devices, e.g., a production unit comprises IoT technology, has Machine-to-Machine (M2M) communication that makes the product better by reducing inefficiencies, and produces faster results.
- ✓ Cost Effective: This merit is actually a combined benefit of the above two merits. Due to easy information access and communication, IoT devices can transmit the data very quickly over a connected component in the network of IoT. So, it saves time compared to traditional data transfer in which it occupied much more time and in that way IoT became a cost effective solution.
- ✓ Automation: It means to manage routine work without any human intervention. IoT helps in business automation and improves the quality product or service. IoT can collect data from the network and perform analytics on it to reveal business insights and opportunities, and thus reduce operational cost. In the automation process, IoT can also predict needs before they arise and take action accordingly to gain business profit.

Demerits:

- Privacy and Security: IoT is an inter-network of things that consists of multiple devices interconnected to each other. So, such interconnection might

increase the risk of any leakage of important data. In this scenario confidential information may not be safe and could be fetched/hacked by someone else easily.

- Complexity: IoT is not only a collection of interconnected heterogeneous devices but also a combination of heterogeneous networks. So, in this environment, a single ambiguity can affect the entire system tremendously. This certainly creates a complicated state of affairs and easily increases complexity.
- Lesser Jobs: Automation is one of the merits of IoT, so the need for manual processing that can be done by human beings will reduce drastically. So, the future of IoT may be one of the reasons for unemployment.
- Dependability: Being complex is one of the demerits of IoT. Due to its intra heterogeneous objects and inter-heterogeneous network connectivity, it also increases dependability of such intra/interconnected object(s)/network(s). So, in case of a bug in the system, there may be a change or collapse of the entire system. Day-by-day IoT technology dominates human lifestyle and thereby increases dependability on IoT technology altogether.

1.2 Technological Evolution Toward IoT

After passing several decades of invention of an electronic device computer, in the 1960s, a communication between two computers was made possible using a computer network. Functioning of the internet commenced after the invention of TCP/IP in the 1980s. Later on, in 1991, the internet became more popular using available WWW. After the invention of www, e-mail, information sharing, and entertainment were introduced on the internet. Interconnectivity of different objects (devices) evolved over the years, and it became the base for technological evolution toward IoT. Web applications became prevalent with evolved network technology resulting in an internetworked ATM. E-commerce was also introduced during this time.

Till 2000, Information and Communication Technology (ICT) provided service related to "anytime", "anywhere" paradigms. It means it provides service connectivity through the internet any time at any place. But in 2000, we witnessed a new era of ubiquity that suggests a new paradigm of connecting "anything" IoT [20]. Mobile internet technology was also formed parallel to evolution on IoT from 2000 to 2010. Due to the invention of mobile internet technology, social networking platforms such as Skype (2003), Facebook (2004), Twitter (2006), and WhatsApp (2009) were also introduced and thereby the users are getting connected via the internet through connecting devices [3, 4].

As shown in Figure 1.2, IoT technology was infant in 2000, and it has matured during the decade that dealt with other pioneering technologies such as RFID, WSN, and M2M communication that underwent revolution in the product automation industries and service industries. After having M2M communication, IoT which is a network of objects, that communicates with each other via different technologies such as Internet, RFID, GPRS, computers, actuators, and mobile phones without or minimal intervention of human beings. The voyage of IoT technology has been continuing in the path of IoT application domain such as Digital Locker, Smart Healthcare, Smart Vehicle, and Smart Cities. Recently, IoT

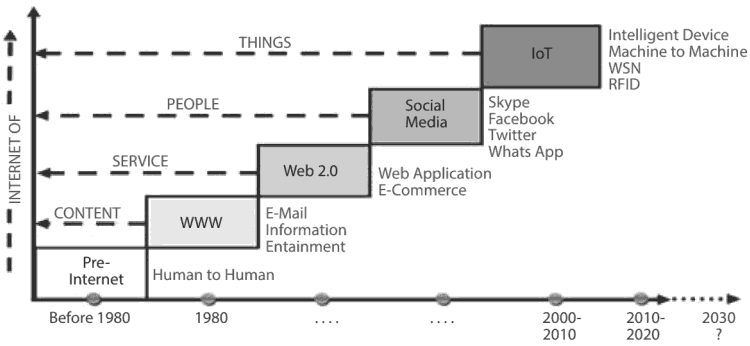


Figure 1.2 Evolution of IoT.

technology emphasizes Smart Dust (a smaller computer than a grain of sand) collaboration with evolved nanotechnology to diagnose problems in the object system or human society.

Thus, the IoT is a paradigm shift in the Internet technology that is rapidly developing by the advancements in other enabling technologies such as sensor networks, mobile devices, wireless communications, networking, and cloud technologies that results into Industrial IoT (IIoT), an application of IoT in industries. So, now, we will discuss those associated technologies which bring such technological revolution in association with IoT.

1.3 IoT-Associated Technology

In Inter-networked of Things, stake holding technologies expect trillions of Sensors, billions of Smart Systems, and millions of applications in near future. There are numerous supportive technologies with IoT to perform smarter than before. IoT Associative Technology can be classified into four sub-topics, namely,

(i) Sensor and Actuators,
(ii) IoT Networking,
(iii) IoT Connectivity Technologies, and
(iv) IoT Communication Protocol.

(i) Sensor and Actuators: Sensor and Actuators are the most essential and core components of the IoT. As per oxford dictionary, the meaning of sensor is "*It is a device which detects or measures a physical property and records, indicates or otherwise responds to it.*" [31]. So, sensors basically sense the physical observable fact around us from an environment. As per the other sources [32], sensors can be defined as "A sensor detects (senses) changes in the ambient conditions or in the state of another device or a system, and forwards or passes this information in a certain manner". According to this definition, a sensor can sense or detect the physical phenomena or measured properties such as temperature, humidity, smoke detection, and

obstacle detection. So, we have different specific sensors that can be used to sense particular properties and cannot be used to sense or to detect, or be insensitive to the other properties surrounding us, i.e., specific physical properties can only be detected by specific sensors not bothering about other properties surrounding us. For example, a temperature sensor can sense heat (temperature) around us and then these sensed values are converted into its equivalent electrical signals.

The smallest change that can be detected and can be measured by a sensor as an output is known as resolution. Based on the output, the sensor can be classified into two categories: Digital Sensor and Analog Sensor. *Analog Sensor* can generate or produce a continuous output signal equivalent to continuous measured property in nature; e.g., temperature, humidity, pressure, and speed are analog quantities. While *Digital Sensor* produces binary output (0 or 1, ON or OFF) signal. So, it generates a non-continuous (discrete) value in the form of bits that combine to gather generated byte as an output. Based on the output data types, sensors can be classified into two major groups: Scalar Sensor and Vector Sensor. *Scalar Sensor* generates output proportional to quantity measured from surroundings without considering its orientation or direction, e.g., physical quantity such as temperature and pressure. *Vector Sensor* generates the output that is proportional to quantity measured as well as its orientation or direction, e.g., physical quantities such as sound and velocity.

Based on sensed information from sensors, actuators basically perform some actions (actuates) on the physical environment. So, here, actuators take actions based on what has been sensed and in that way controls a system that can be acted upon an environment. In this context, the actuators require some control signal and source of energy to function further. So, when actuators receive such control signals, they convert the energy into mechanical motion. Based on their functional domains, we have three broad categories of actuators such as pressure-based actuators (hydraulic and pneumatic), electric-based actuators (electrical, thermal, and magnetic), and mechanical-based actuators. Other than these types of actuators, other popular actuators are used in industries. Agriculture uses Soft actuators. Soft actuators are polymer-based actuators designed to handle delicate objects and used in robotics.

"*Transducer*" is another associative term which can be used for both Sensors and Actuators [33]. So, actuators sense the surroundings in the form of information and are converted into electrical signals; such control signals are received by actuators and action is taken accordingly. For example, in "soil moisture and water level monitoring application", agriculture soil water/moisture level in a farm is sensed by specific sensors, is converted into electrical signal, and is provided to the actuator as "solenoid valve". Solenoid valves consist of a mechanism that allows or stops the water flow. So, depending on the electrical signal received from the sensor (water/moisture level), this solenoid valve as an actuator can actuate, i.e., flow water or stop water.

(ii) IoT Networking: IoT Network consists of several components such as Device (The Thing), Local Network, Internet, Backend services, and Applications. Here, in case of "Device", it consists of a collection of sensors and actuators that can act as one component in the entire IoT Network. These become different nodes in the IoT Network that can be communicated with each other. As shown in Figure 1.3, a node in IoT Network can be communicated with other target node via another component of IoT network, i.e., Local Network. If target node does not belong to the local network, IoT network will search it through another component of IoT network, i.e., Internet. In Backend services, the data may be received from local networks or from the internet and perform complex analysis using different machine learning algorithms.

Such result generated after complex analysis is given to applications that serve as an output of IoT Network. Thus, IoT is a very complex system that involves things (sensors and actuators), local area network, wide area network (internet), machine learning, and analysis algorithms which act mutually into one system entity.

Such result generated after complex analysis is given to applications that serve as an output of IoT Network. Thus, IoT is a very complex system that involves things (sensors and actuators), local area network, wide area network (internet), machine learning, and algorithms which act mutually into one system entity.

So, to perform function through IoT we need more associative technology such as Bigdata, M2M communication, cloud computing, Cyber Physical System (CPS), 3G/4G/5G, and Internet of Vehicles (IoV). To perform suitable communication among such heterogeneous technologies and devices, we need to deal with certain *challenges* of IoT. They are securities, interoperability, scalability, energy efficiency, and interfacing. IoT connectivity technologies are involved in IoT communication to execute it properly. They are as per the sub topics given below.

(iii) IoT Connectivity Technology: Connectivity among devices is fundamental when we think about the IoT. There are several IoT connectivity technologies in the form of communication protocols that utilize IoT networks to perform communication between IoT devices (Things). IoT service offering protocols such as RFID (Radio Frequency Identification), CoAP (Constrained Application protocol), XMPP (Extensible Messaging

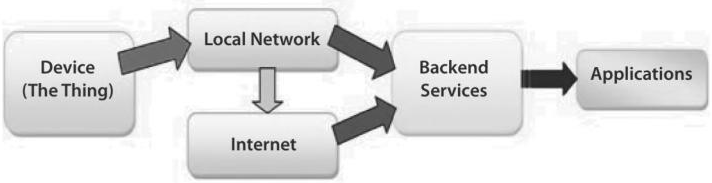


Figure 1.3 IoT networking.

Presence Protocol), MQTT (Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol), and 6LoPAN (IPv6 over Low-Power Wireless Personal Area Networks) are basically utilized to establish connectivity between IoT devices in IoT network.

RFID stands for Radio Frequency Identification that is used widely in shopping malls as a system whole. RFID system consists of RFID tag, RFID reader, and RFID software. RFID tag is covered by a hard jacket that consists of integrated circuit and antenna and stores digitally encoded data. RFID tags are categorized into Active Tag (own power supply) and Passive Tag (dependent for power supply). RFID reader reads from the tag and transfers data to RFID software for further processes to operate.

CoAP, as per its name Constrained Application Protocol [13], is utilized for web transfer just as http but in constrained networks resources environment such as limited computational resources, limited bandwidth and limited power supply in IoT. CoAP in IoT network functions as a session layer and an application layer. CoAP is designed for M2M communication and uses a request-response model for two connected endpoints (objects) in the IoT network.

XMPP stands for Extensible Messaging and Presence Protocol [06], an open standard XML (extensible markup language)–based middleware protocol that is used for real-time structured data exchange. XMPP uses decentralized client-server architecture which means the central server is not located for message transfer. So, in this context, XMPP provides flexibility in sustaining interoperability between different things (objects), between diverse systems, and between heterogeneous protocols in the IoT network. XMPP does not support text-based communication.

MQTT is a Message Queuing Telemetry Transport protocol [7], publish-subscribe–based ISO standard protocol. So, in this protocol, publisher publishes the data that can be utilized by the subscriber and this phenomenon creates this protocol as a lightweight protocol that can be used in combination with TCP/IP protocol. In MQTT, there is a central entity known as "broker" which is responsible for transferring messages from sender to receiver. Here, client publishes a message to the broker including topic (routing information for broker). Based on the matching topic, the broker delivers the message to the client. So, in this architecture, client does not know the real message passing entity, this feature provides a highly scalable solution independent of data producer and data consumer. MQTT is used by Microsoft Azure, Amazon Web Services, Facebook Messenger, and Adafruit for providing various services.

AMQP stands for Advanced Message Queuing Protocol [14] and is ISO/IEC-based open standard protocol for passing business messages between different business applications or organizations. At the time of passing business messages, AMQP is persistent and provides three different types of message delivery guarantees. They are At-most-once (message delivered

once or never), At-least-once (message certainly delivered may be multiple times), and Exactly-once (certainly delivered and only once).

6LoPAN is an IPv6 over Low-Power Wireless Personal Area Networks [15]. Due to large components involved in the IoT network, unique address identification can be done through IPv6 (64 bits) address protocol instead of IPv4 (16 bits) address protocol. This protocol provides transmission of data wirelessly with limited data processing potential in PAN. So, as per its name, it permits low-powered devices to connect to the internet which is also a basic characteristic of IoT networks.

(iv) IoT Communication Protocol: Other well-known communication protocols that require to perform communication in IoT network are IEEE 802.15.4, Zigbee, Z-Wave, Wireless-HART (wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol), Near-Field Communication (NFC), and Bluetooth as given below.

IEEE 802.15.4 is an extensively used standard protocol for establishing communication in the IoT network [9, 10]. It provides a framework for lower layers such as physical layer and Mac layer to a small range of Personal Area Network (PAN) and Wireless Personal Area Network (WPAN) that generally range from 10 to 75 meters in the environment of low-power, low-speed, and low-cost requirements. It uses star and peer-to-peer network topologies for establishing communication between neighboring devices in the IoT network.

Zigbee is an enhanced version of IEEE 802.15.4 that functions on top of layer 1 and layer 2 of IEEE 802.15.4 in layer 3 and onwards [11, 12]. So, Zigbee uses the MAC layer to the application layer in the IoT Network. Zigbee is basically used for Wireless Sensor Network (WSN) and supports stat and mesh topology. In Ad-hoc network, Zigbee utilizes Ad-hoc On-demand Distance Vector (AODV) Protocol for broadcasting a route request to all its immediate neighbors. Such neighbors spread this message to their neighbors and, in that way, messages can be spread all the way through the IoT network. One of the important applications utilized by Zigbee is "Building Automation". Other applications are healthcare monitoring, home energy monitoring, LED lighting monitoring, telecom services, and many more.

Z-Wave is a well-known protocol for home automation to do different functions using various IoT devices. It functions on mesh topology that can have up to 232 nodes (devices) in a network and uses radio frequency for communication, i.e., signaling and controlling of home automation IoT devices. In a home, there is a Z-Wave controller that controls the signal communication with existing other Z-Wave nodes (devices). Such Z-Wave devices may communicate directly with each other or they can communicate via Z-Wave controller in smart home automation systems.

Wireless-HART is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol [16] that is developed

for networked smart field devices. IoT implementation and cost of performing communication between IoT devices will be cheaper and easier using HART. There are certain differences between physical HART and wireless HART in the context of physical layer, data link layer, and network layer. HART physical layer utilizes IEEE 802.15.4 protocol. HART data link layer has a provision of a super frame that ensures suitable communication between different IoT devices (nodes) of the IoT network. Wireless HART network layer uses mesh topology for communication in IoT networking. Wireless HART protocol network layer can be composed of OSI Network layer, transport layer, and session layer. HART application layer is responsible for generating responses by extracting commands from messages and executing them. So, the basic difference between Wireless HART and Zigbee is that Zigbee hops when the entire network hops but Wireless HART hops after every message.

Near-Field Communication (NFC) is designed for use of devices in its close proximity and uses magnetic induction principle just as RFID [17]. Based on power/energy resource availability, NFC has two types, viz., Active NFC and Passive NFC. Active NFC does not depend on external power/energy resources and Passive NFC depends on external power/energy resources. Like RFID, NFC also has three components: reader, tag, and software. NFC reader creates magnetic fields using electric current that connects the physical space between these two devices, NFC reader and NFC tag, and can transmit encoded information from NFC tags such as identification number. NFC can be operated in three different modes much as peer-to-peer, read/write and card emulation. For example, in peer-to-peer mode, two smartphones can communicate with each other. In read/write mode, one active and one passive device is involved to perform communication and in card emulation NFC can be used for contactless credit card operation.

Bluetooth is a wireless short range communication technology that is heavily used in establishing communication in IoT network devices in PANs [18]. Bluetooth can be utilized to perform communication between two smart phones for transferring data to short range. Bluetooth uses ad-hoc technology known as Ad-hoc Piconets. Connection establishment in Bluetooth can be possible in sequence using three different phases such as Inquiry, Paging, and Connection. In the "Inquiry" phase, Bluetooth devices discover other Bluetooth devices near it. After finding a Bluetooth device nearer to the current device, in this second phase "paging", connection can be established between these two devices. In the third phase of "connection", either devices can actively participate in the network or enter into low-power sleep mode.

After discussing IoT associative technology such Sensor and Actuators, IoT Networking, IoT connecting technology, and IoT communication protocol, the important characteristic of IoT devices and technologies that make all this possible is "Interoperability in IoT" as discussed in the next topic.

1.4 Interoperability in IoT

In IoT, many heterogeneous devices, protocols, operating systems have to work together to fulfill objectives. This heterogeneity is one of the major concerns when we perform communication in the world of IoT as it requires not only anytime, anywhere but also anything enabled to communicate. "Interoperability" is a characteristic of a product or system whose interfaces are completely understood to work with other products or systems without any limitations. Interoperability is must when we would like to communicate in the era of IoT that contains heterogeneous devices [19]. So, by maintaining interoperability in the IoT network, we can have exchange of data and service in a seamless manner. In this seamless exchange of data and service, many elements are involved and perform the communication such as physical objects can communicate with other physical objects.

As per the overall goal of IoT, anytime anywhere anything (device) can be communicated with other devices, i.e., can do Device-to-Device (D2D) communication. More than these types of communication, others such as Device-to-Machine (D2M) communication, M2M communication should also be performed seamlessly in the IoT network. Hence, in this situation, the IoT network has to deal with many types of heterogeneity such as heterogeneity of different wired and wireless communication protocols. Moreover, different programming languages are used for different platforms as well as different hardwares that also vary different standards and support different languages and communication protocols. So, if we would like to perform seamless communication between such corel, heterogeneous connected components, protocols, languages, operating systems, databases, and hardwares, then interoperability among them is a must.

There are basically two types of Interoperability such as User Interoperability and Device Interoperability. User Interoperability is an interoperability problem between user and device(s) and Device Interoperability is an interoperability problem between two different devices. User interoperability problems occur when remotely located users would like to communicate with other device(s) whose product id may be written in different language, there may be differences in user syntaxes, differences in user semantics, as well as differences in user specification for those devices. So, all these types of complex veracity leads to create a simple IoT problem into a complex one that falls under the problem of interoperability.

To resolve such user *syntax interoperability* problems worldwide, there are different solutions that provide unique device identification addresses to devices such as Electronic Product Codes (EPC), Universal Product Code (UPC), Uniform Resource Locator (URL), and IP addresses IPv6. For resolving *syntactic interoperability* problems there are different approaches such as Open standard protocol (IEEE 802.15.4, IEEE 802.15.1, and Wireless HART), Closed standard protocol (Z-Wave), Service Oriented Computing (SOC), and web services. But all these approaches have the problem of heterogeneity and, therefore, incompatible with each other to perform communication. So, we have certain middleware technologies such as Universal Middleware Bridge (UMB) that resolve such devices interoperability problems that have been generated due to heterogeneity amongst them. Thus, in this topic we have discussed IoT which is surrounded by heterogeneity problems, which can be resolved using interoperability features. The next topic explains about the programming technologies concerned with IoT.

1.5 Programming Technologies in IoT

The programming technologies associated with IoT such as Arduino programming, Python programming, and Raspberry Pi are well known. *Arduino* programming can be done in consultation with the Arduino UNO board to accept analog and digital signals as input and generate desired output. *Python* is a lightweight programming language that is very much popular for IoT application development. *Raspberry Pi* is powerful compared to *Arduino* in terms of memory capacity and processing power. *Raspberry Pi* is a single-board, low-cost computer that provides easy access using GUI.

1.5.1 Arduino

Arduino is low resource consuming and cheaper in cost. Due to these two characteristics, it is popular worldwide for implementing the IoT. As shown in Figure 1.4, Arduino is an open source programmable board with a built-in microcontroller and the software (IDE). So, using this Arduino board, we can have input as analog or digital signals and produce digital signal as an output and there is no need to have a separate programmer to program it like traditional microprocessor 8051 and 8085. To program the Arduino microcontroller board, open source software of Arduino IDE is utilized using C or C++ programming language. IDE can be downloaded from Arduino's official website [22].

To do programming in the Arduino board, install Arduino IDE. Now switch on the Arduino board by attaching it with USB cable to PC and launch Arduino IDE. Using the TOOLS option of this IDE, set BOARD type and PORT type. Program coded in Arduino is known as "sketch". So, go to the file menu and click on "Create New Sketch" to write a new program in Arduino. Sketch structure in the Arduino IDE can be divided in two major functions: Setup() and Loop(). Setup() function is just like the main() of C/C++ in which we can declare input/output variables and pinmodes can also be declared over here. As per the name, Loop() function is used for iterating the instruction(s) written under it. Using the

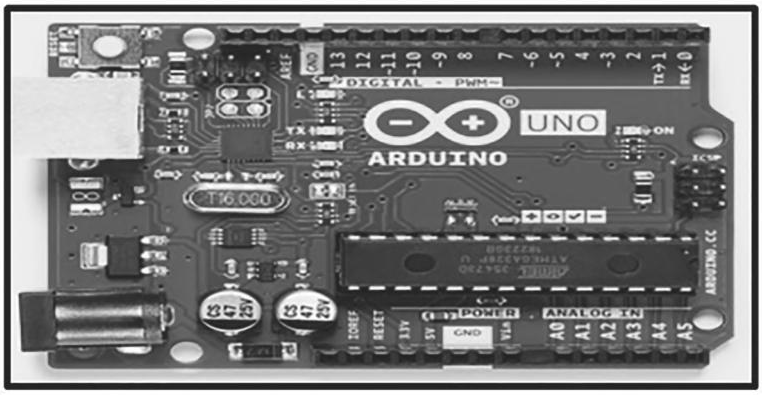


Figure 1.4 Arduino UNO board [21].

"pinMode()" function of the Arduino IDE library, we can have the syntax of this function as given below. The common functions of the Arduino library are as given in Table 1.1.

Table 1.1 Arduino function and its description.

Function	Function Description
pinMode(*pin, Mode*)	Configure the input/output pin(s) with its pin number in the arduino board. *pin* = pin number on Arduino board, *Mode* = INPUT/ OUTPUT
digitalWriter()	Write digital pin value (HIGH/LOW)
analogRead()	Read from analog input pin
Delay()	Provides a delay of specified time in milliseconds

Using the above common function, we can write down a program in Arduino IDE that is used for "Blinking LED". To perform this practical on an Arduino board, we require several objects/entities as hardware such as an Arduino micro-controller board, USB connector, LED, respective capacity of resistor, bread board, connecting wires, and as a software Arduino IDE as shown in Table 1.2.

Table 1.2 Arduino programming requirement.

Activity	Hardware Side	Software Side
Prerequisite	Arduino micro-controller board, USB connector, LED, respective capacity of Registers, Bread board, Connecting wires	Arduino IDE
Process	✓ Using connecting wires, set LED on breadboard and connect it to Arduino Using USB connector, connects Arduino board to PC	• Select Board and Port type • Write equivalent Sketch in Arduino IDE Verify sketch and upload it

Sample Arduino "Sketch" for Blinking LED:

```
void Setup( )
{
        pinMode(12, OUTPUT);          // set arduino pin number 12 for digital output
}
void Loop( )
{
        DigitalWriter(12,HIGH);       // Turn ON the LED
        Delay(500);                   // wait for 500 millisecond = 0.5 second
        DigitalWriter(12,LOW);        //Turn OFF the LED
        Delay(500);                   // wait for 500 millisecond = 0.5 second
}
```

1.5.2 Raspberry Pi

As shown in Figure 1.5 Raspberry Pi is a low-cost, single-board, palm-size computer that provides easy access. Raspberry Pi has higher processing capabilities and more features compared to Arduino [23]. So, such programming technology is better when we have more data for processing such as image and multimedia sensor data processing. To do so, we can download freely available Raspberry Pi–based operating systems which are GUI-based systems. For example, Raspbian and Noobs are officially supported OS for Raspberry Pi. Other operating systems that also support this technology are Windows 10 core, Snappy Ubuntu code, Ubuntu Mate, Pinet, and Risc OS. Supported programming languages for Raspberry Pi are C, C++, JAVA, Python, and Ruby. The following Raspberry device can act as a server as well as a node in IoT networking. So, we can create an interactive environment using such a network of connected devices.

We can have an IoT-based system that can perform different tasks such as collecting data from connected sensors of the network, send such received data to a remote machine or server, process the data, and respond accordingly in the IoT network. For example, suppose we have a digital DHT (Digital Humidity Temperature) sensor that senses the data of the surrounding environment. Collected data is then transferred to server and saved on server for further processing and after processing such information is updated on screen based on responses available from the network.

To do so, we require a digital humidity temperature sensor, register, jumper wires, and Raspberry Pi unit. As shown in Figure 1.6, DHT sensors have four pins numbered as 1, 2, 3, and 4. Pin 1 used for power supply of 3.3 to 5.0 V, pin 2 used for data, pin 3 is null, and pin 4 utilized for ground. So, connect pin 1 of DHT sensor to the 3.3V pin of Raspberry Pi, connect pin 2 of DHT sensor to any input pin of Raspberry Pi and connect pin 4 of DHT sensor to ground of Raspberry Pi. So, after establishing connection of DHT sensor with Raspberry Pi, reading data from sensor using ".read_retry" method consists in "Adafruit" library of DHT22 sensor. To transfer data to the server, we can establish a connection between client and server, send data from client to server and then save the data in a particular file at server

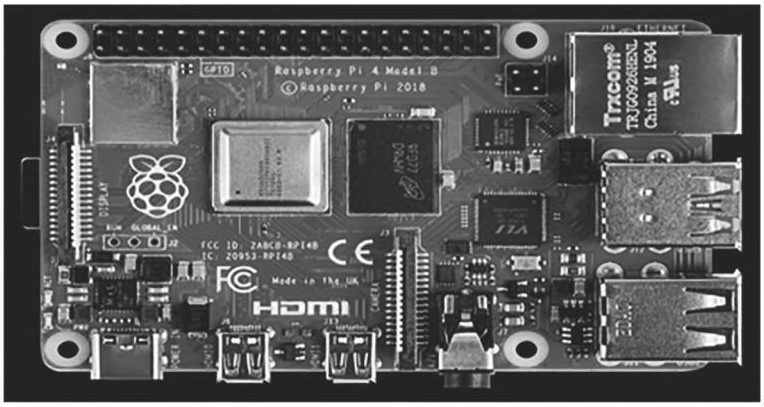


Figure 1.5 Raspberry Pi 4 [24].

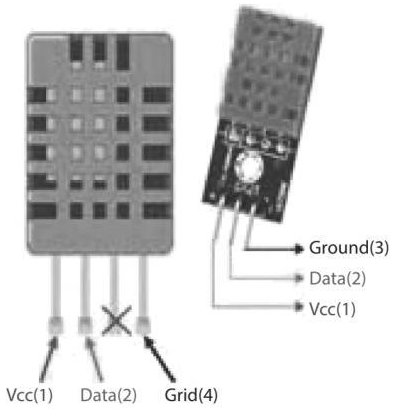


Figure 1.6 DHT sensor [29].

end in the form of a log file. Data processing is done at server end that may include filtering and plotting of data. Due to lack of data, there may be a chance of incomplete or corrupted data so to overcome such data, and we need preprocessing activity such as cleansing and to do so we use filtering over here. To plot the 2D data at the server end, a Python library MATPLOTLIB can be utilized.

In this way, using a DHT sensor with Raspberry Pi, we can monitor the value of humidity and temperature on screen with the help of GUI. Even we can extend/update the script and instruct the rotary motor as an actuator to actuate (start fan) when certain room temperature increases. So, these are some of the modest applications of IoT in real-world environments that can be implemented using Raspberry Pi.

1.5.3 Python

As a lightweight versatile scripting programming language, Python is very much popular and useful in IoT-based application development [25]. It provides some kind of relaxed environment, i.e., it does not follow strict rules. Python-Integrated Development Environment (IDE) provides several modules and libraries, using which one can establish connectivity with many hardware and also compatible with multiple OS such as windows, Linux, and MAC. Well-known Python IDEs are Spyder and PyCharm.

To perform file operation in Python, we do not require any separate library, and it is an in-built function such as open(), read(), write(), and close(). Python supports various file formats to perform such operations like .Txt file and .CSV file. This feature makes data management easier using python programming language. If our data file is of the type of image, then we have a Python Image Library (PIL) to do the process with such a file. In this library, there are famous functions/methods like open(), show(), resize(), rotate(), print(), and convert() to do various tasks on such images that are contained in an image file.

Python also supports client-server architecture model and provides necessary network services to it. Socket programming in Python allows us to implement clients and servers for connection oriented as well as connection less protocols. In socket programming of

Python, we have to import "socket" and "sys" libraries that contain well-known and most utilized functions for example connect(), send(), and listen() using which one can establish connection between clients (IoT nodes) and server. Python has also a separate library that provides and deals with a specific application level network protocol(s).

Thus, Python is a versatile object oriented programming language that provides an easy environment in open source community software for the development of IoT-based applications.

1.6 IoT Applications

With the collaboration and co-operation of other technology involved with IoT, it has vast scope in various IoT-based applications such as Smart Home, Smart Healthcare, Smart Transportation, Smart Asset Management, and Smart Farm [26]. Such applications will create a paradigm shift in the traditional lifestyle of human beings and that is why nowadays the popularity of IoT is much more than other existing technologies. Some of the well-known IoT applications are as given below.

Smart Home
Smart home as an IoT application contains features like integration of various IoT-enabled devices, provides securities amongst them, and enables networking using central controlled devices and its related security features that adapt a traditional home into technically enriched sophisticated home. Such IoT-enabled devices monitor some important aspects for home such as remote air conditioning, heating, and ventilation management using smart phones. It also performs the operation management by communicating with different IoT-enabled devices of home like IoT-enabled fan, tube light, oven, and washing machine.

Smart Healthcare
Such smart healthcare applications are also known as the Internet of Medical Things (IoMT). Its popular applications are "Remote Health Monitoring" and "Emergency Notifications System" [27]. There are many devices that can monitor the number of health parameters of human beings. IoT-enabled devices, by collaborating communication with medical manifesto, can monitor the heartbeat and blood pressure and, with proper medical surgery, can also act as pacemaker. "Smart Bed" is an instrumental bed which maintains a patient's regular checkups without any human intervention (nurse). Moreover, such smart beds can also be connected using smart sensors that can acquire information from the patient end and analyze and transmit them to smart home objects connected to this system. To monitor the well-being of senior citizens, smart sensors can also be medically equipped within living spaces of human beings.

Smart Transportation
In different aspects of the transportation system, IoT is helpful in doing things more smartly than done earlier. IoT-enabled devices can be equipped with vehicles, infrastructures, drivers and other human beings involved in transporting activities and can play the role of a monitor or supervisor. So, logistics, smart traffic control, vehicle control, and fleet

management are several well-known applications of the Smart Transportation segment. During transportation of any goods container, it can be handled by monitoring the real-time location of the container, the status of the container (open/close), and how the container can be handled throughout the journey. So, such smart tracking can provide security features to that container and thereby minimize the theft risk and maximize the possibilities of recovering stolen material.

Smart Asset Management

Asset management is one the oldest problems faced by many industries. Asset is basically an instrument or a device that may be cheap or priceless, that may be located indoor or outdoor. So, in case of an emergency, it is often a problem finding/tracking its location in the organization. IoT can provide solutions toward pinpointing the asset's exact location within a short span of time. For example, in hospitals, there are many assets such as medical instruments, scanning machines, and healthcare monitors loosely coupled with each other. So, by using IoT-enabled solutions, one can correlate them technically and upload the data on cloud to monitor its future activities such as scheduled maintenance without intervention of human beings.

There are many other domains too in which IoT can be applied to operate things better and smarter such as Smart Retailing, Smart Inventory Management, Smart Tracking, and Smart Cargo Management. In industries, the IIoT can be applied. That is one of the reasons for Industrial Revolution 4.0. So, in the context of industries IoT, we have other broad domains in which IoT can be served. Such domains are Smart Factory, Food Industries, Plant securities and safety, Oil Chemical and Pharmaceutical Industries, Unmanned Auto Vehicle industries (UAVs), and many more. The domain of agriculture also utilizes IoT facilities in different sub-applications and converts the agriculture farm into a Smart Farm. So, in the next sub-topic, we shall discuss how premium facilities can be developed in traditional farms and how one can use IoT technology to convert a farm into a Smart component of sustainable agriculture.

Smart Farm—A Paradigm Shift in Sustainable Agriculture

Smart Farm is an IoT application that gives leverage to the farmer community to do many farm level tasks using IoT without human intervention or minimal human intervention. Smart Farm consists of a variety of functions such as water level management, soil fertility management, pesticides control, and many more. IoT-enabled devices can be useful to fulfill the basic communication functionality that result into performing smart work in the agriculture domain at farm level.

In future, smart farms can have the facilities such as soil moisture and water level monitoring, automated irrigation system, automated sowing and weeding system, automated organic waste management system, automated environment monitoring system, and soil micronutrients monitoring system as shown in Figure 1.7.

✓ Out of these systems, IIT Kharagpur, India, developed an automated irrigation system, "AgriSens" that focused on Smart Water Management using IoT [29]. AgriSens provides automatic irrigation and remote monitoring and controlling. Architecture of this system has basically three layers: sensing layer, processing layer, and application layer. Sensing layer deals with

Figure 1.7 Future smart farm [28].

functionalities of different sensors such as soil moisture sensor and water level sensor that receive information from surrounding and pass to its cluster head. Such received information transfer from cluster head to remote server for further processing and analytics will be done at different application sides on such processed data to get the ultimate result. Such analytics results decide what should be the next step to follow and accordingly sends signal to/stop signal from actuators (e.g., water pump motor) to actuate (start/stop).

- ✓ In other agriculture domains, IoT applications such as *environment monitoring systems* will sense the environmental data such as level of carbon dioxide, level of nitrogen, and level of oxygen in the surroundings and alert if it goes beyond the lower level. At this time, it checks crop-based requirements accordingly and informs the remotely existed farmer community so that they can take action accordingly.
- ✓ In *automated seed sowing systems*, there are sensor mounted tractors that can monitor the shift of the tractor and accordingly dig soil and another sensor pushes seed into the soil. So, using such sensor-based sowing automation, the farmer community can get proper inline and depth seed sowing that can be easily maintained during its production phase and thereby increasing the overall production of the related crop.
- ✓ *Soil fertility monitoring systems* will basically consist of different sensors that can sense different micronutrients from soil. In its processing part, it compares with related crop ideal requirements, and if a gap is found beyond threshold, it sends an alert to a remotely existing famer on his smart device.

So, by utilizing IoT applications in the agriculture domain, specifically at farm level as mentioned by above various IoT-based applications, our traditional farm can act as a Smart Farm that helps the farmer community to increase crop production quality and quantity and thereby achieve their overall goal of profit making with less sweat.

Conclusion

This chapter explains the Introduction of IoT and its basics. It covers Technological Evolution and Associate Technology such as IoT network and communication protocols. In the voyage of this chapter, it also explains the "Interoperability" as a solution of the serious issue of heterogeneity in IoT. This chapter moreover discusses some practical aspects in IoT programming using Arduino, Raspberry Pi, and Python programming language. It also explains IoT applications with a splendidly useful application of IoT in the agriculture domain such as "Smart Farm". The main aim of this chapter is to draw attention and interest of the reader toward the IoT domain and induce him/her toward this domain which may result into innovative ideas in this domain.

References

1. Tripathy, B.K. and Anuradha, J. (Eds.), *Internet of Things (Iot) Technologies, Applications, Challenges, and Solutions*, pp. 41–59, CRC Press, Taylor and Francies Group Ch-3, London, 2018.
2. Patel, K.K. and Patel, S.M., Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *Int. J. Eng. Sci. Comput.*, 6, 5, 6122–6131, May 2016.
3. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S. *et al.*, Internet of Things Strategic Research Agenda, in: *Ch.02 - Internet of Things-Global Technological and Societal Trends*, River Publishers, Denmark, 2011.
4. *Internet of Things: Evolution and technologies from a security perspective*, vol. 54, p. 101728, Elsevier - Sustainable Cities and Society, Manchester, U.K., March 2020, https://doi.org/10.1016/j.scs.2019.101728.
5. Silva, B.N., Khan, M., Han, K., *Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges*, pp. 205–220, Taylor and Fransis Online Published online, Howick Place, London, 08 Feb 2017, https://doi.org/10.1080/02564602.2016.1276416.
6. Learning Internet of Things, in: *Chapter – 06 The XMPP Protocol*, pp. 125–162, Peter Waher, PACKT Publishing, Birmingham – Mumbai, 2015.
7. Learning Internet of Things, in: *Chapter – 05 The XMPP Protocol*, pp. 107–123, Peter Waher, PACKT Publishing, Birmingham – Mumbai, 2015.
8. *The Evolution of the Internet of Things*, White Paper, Jim Chase, Texas Instruments, Dallas, Texas, September 2013.
9. Poole, I., IEEE 802.15.4 Technology and Standard, online: URL: https://www.radio-electronic.com/info/wireless/ieee-802-15-4/wireless-standard-technology.php. 2013.
10. Fenzel, L., Difference between IEEE 802.15.4 and Zigbee online URL: htts://www.elecronic-design.com/what-s-different-between-ieee-802154-and-zigbee-wireless.
11. Agarwal, T., Zigbee wireless technology Architecture and Application. Online URL https://https:elprocus.com/what-is-zigbee-wireless-technology-architecture-and-its-application.
12. Acosta, G., The Zigbee Protocol online URL: https://www.netguru.com/codestories/the-zigbee-protocol.
13. Shelby, Z., Hartke, K., Bormann, C., The Constrained Application Protocol (COAP), in: *Internet Engineering Task Force (IETF)*, Standard Track, Bremen, Germany, 2014.
14. Tezer, O.S., *An Advanced messaging queuing protocol walkthrough*, Digital Ocean–Online, 2013.

15. Sulthana, M.R., A Novel Location Base Routine Protocol for 6LoWPAN, a developer cloud environment.
16. Feng, A., A Survey of Protocols and Standards for Internet of Things. *Adv. Comput. Commun.*, 1, 1, pp. 1–21, 2011.
17. Egan, M., *What is NFC? How to use NFC on your smartphones*, Techadvisor, (online), Euston Road, London, 2015.
18. Tutorialspoint – Online, Wireless Communication – Bluetooth.
19. Čolakovića, A. and Hadžialićb, M., *Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues*, vol. 144, pp. 17–39, Elsevier - Computer Networks, Amsterdam, The Netherlands, 24 October 2018.
20. Gomathi, R.M., Hari Satya Krishna, G., Brumancia, E., Mistica Dhas, Y., A Survey on IoT Technologies, Evolution and Architecture. *2nd International Conference on Computer, Communication, and Signal Processing (ICCCSP 2018)*.
21. Arduino Store, Online https://store.arduino.cc/usa/arduino-uno-rev3 (image download).
22. Arduino Integrated Development Environment-IDE https://www.arduino.cc/en/Main/Software
23. Learning Internet of Things, in: *Chapter – 01 Preparing our IoT Project*, pp. 11–33, Peter Waher, PACKT Publishing, Birmingham – Mumbai, 2015.
24. Raspberry Official Website - https://www.raspberrypi.org/downloads/ (for image and software)
25. Official Web site – Python - https://www.python.org (for documentation and download)
26. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S. *et al.*, Internet of Things Strategic Research Agenda, in: *Ch.03 - Internet of Things-Global Technological and Societal Trends*, River Publishers, Denmark, 2011.
27. Le, D.-N., Van Le, C., Tromp, J.G., Nguyen, G.N. (Eds.), *Emerging technologies for health and medicine_ virtual reality, augmented reality, artificial intelligence, internet of things, robotics, industry 4.0*, Scrivener Publishing, Wiley. October 2018.
28. Agriculture 3.0 or (smart) agroecology, online: https://www.grain.org/en/article/6280-agriculture-3-0/-or-smart-agroecolog
29. AgriSens:Development of Sensor based Networking System for Improved Water Management for Irrigated Crops, A Project Funded By MHRD, Govt. of India, Undertaken by SWAN, department of CSE & AGFE, IIT Kharagpur, official website: www.iitkgp.ac.in
30. http://www.gartner.com/it-glossary/internet-of-things/ - visited on 22/07/2020 at 5.30 p.m.
31. https://en.oxforddictionaries.com/definition/sensor - visited on 26/07/2020 at 4 p.m.
32. https://businessdictionary.com/definition/sensor.html - visited on 26/07/2020 at 4.30 p.m.
33. http://www.electronics-tutorials.ws/io/io_1.html - visited on 26/07/2020 at 4.30 p.m.

2

AI for Wireless Network Optimization: Challenges and Opportunities

Murad Abusubaih

Department of Electrical Engineering, Palestine Polytechnic University, Hebron, Palestine

Abstract

Nowadays, Artificial Intelligence (AI) and Machine Learning (ML) are gaining increased attention. The huge amount of information coupled with a plethora of multimedia applications have posed a great challenge to scientists and engineers to handle the big data and manage various resources. All of this prompted researchers to think of innovative ways to make best use of AI and its tools to address existing and emerging problems in the field of data science and data networks. This had an impact on developing the concept of self-organized networks and systems.

This chapter discusses a state-of-art of AI concepts and tools applied to wireless networking. We firstly introduce the AI concepts. We review self-organizing and cognitive networks. Then, we introduce the ML approach. We discuss how AI and ML would contribute to the management of wireless networks as well as the optimization of their operation. To help researchers gain a focused knowledge on the role of AI concepts in facilitating solutions to various problems in wireless networks, we discuss different areas and challenges where AI and ML have been used effectively to overcome those challenges.

Keywords: Artificial intelligence, machine learning, wireless networks, cognitive networks

2.1 Introduction to AI

Artificial Intelligence (AI) is a field of science that is constantly evolving and accelerating. It has recently witnessed great momentum in being one of the scientific fields that have become affecting all sciences. AI has transformed the research path to new directions in order to provide effective solutions to many problems facing all science and engineering fields. In fact, the concepts of AI go back to the 1940s and 1950s, when scientists from different disciplines explored the possibilities of artificial brains and defined machine intelligence.

AI systems can be divided into three types: analytical AI, human-inspired AI, and humanized AI. Analytical AI has characteristics compatible only with cognitive intelligence, where new knowledge and decisions are generated through learning and based on previous experience. Human-inspired AI is a mix of cognitive and emotional intelligence.

Email: murads@ppu.edu

Pardeep Kumar, Vishal Jain and Vasaki Ponnusamy (eds.) The Smart Cyber Ecosystem for Sustainable Development, (25–56) © 2021 Scrivener Publishing LLC

Human emotions are understood, in addition to the cognitive elements, and then used in determining decisions. Humanized AI uses cognitive, emotional, and social intelligence, capable of being self-conscious, and self-aware in interacting with others.

The basic idea of AI is based on a simulation process of the interaction of data in human thinking, trying to understand human intelligence and then developing intelligent machines. AI has the ability to access objects, categories, their characteristics, and the relationships between them in order to apply knowledge engineering. AI aims to expand the capabilities of mankind in carrying out various tasks and consolidate the principles of intelligence in machines and devices in order to save time and effort and to provide distinguished services in various fields. Nowadays, we are witnessing the emerging of many smart devices in different fields, especially in engineering and medical sciences. Specific examples are computer vision, natural language processing, the science of cognition and reasoning, robotics, game theory, and machine learning (ML). Intelligent machines would have some of the capabilities related to human thinking in dealing with problems and make appropriate decisions for any event that may appear during machine operation.

It is known that existing networks lack the intelligence needed to support future next-generation networks that are expected to be self-adaptive. Mobile networks consist of a large number of elements that interact with each other, creating a great complexity in the system that operates these elements together. Wireless networks constitute one of the most important areas that aspire to benefit and consolidate the principles of AI in order to adopt solutions to many problems appeared previously and appear currently in this field. Although we observe a great revolution in scientific research that relies on AI tools to develop and design wireless networks, applying AI approaches to network planning, design, and operations is still in the early stages. This is due to the fact that existing network architectures are not suited to the AI-enabled networks. Researchers are looking not only at the use of AI-based solutions to current problems, but noticeable research have returned to previous problems and tried to develop AI-based solutions. Later in this chapter, we will discuss recent research issues that can benefit from and exploit the principles of AI and ML.

The main research directions that use the AI paradigm are as follows:

- Expert Systems
  An expert system is a software system that relies on human expertise for decision-making. It is appropriate to deal with problems that involve incomplete information or big data.
- Machine Learning
  ML relies primarily on how the computer simulates the behavior of human learning, then restructures the knowledge and acquires new skills to continuously improve performance.
- Pattern Recognition
  The concept of pattern recognition is applied to process monitoring that assumes a relationship between data patterns. The research in pattern recognition includes two main issues: the first relates to object perception and the second relates to determining the category to which the object belongs.
- Neural Networks
  The concept of artificial neural networks is based on non-linear mapping between the system's inputs and outputs. It consists of interconnected neurons

arranged in layers. The layers are connected, allowing signals to propagate from the layers' inputs across the network. A neural network stores data, learns from it, and improves its capabilities to sort new data.

- Deep Learning
  Deep learning is the application of the concept of artificial neural networks to learning tasks that contain more than one hidden layer. It is part of a larger group of ML techniques that are based on representations of learning data. Deep learning concepts come from artificial neural network research, which opened a window to a new field of ML. Concepts of deep learning have been applied in various fields including computer vision, speech recognition systems, natural language processing systems, voice recognition systems, social networking systems, automatic translation systems, and bioinformatics systems, where the adoption of deep learning techniques has led to more effective results as compared to human experience and previous systems.

2.2 Self-Organizing Networks

The primary goal of mobile networks is to connect mobile phone users together as well as to the Internet. Therefore, wireless network operators install large number of base stations or access points in the regions that will be covered. Each base station or access point covers a specific geographical area called a cell. Mobile networks allow users to transparently move between cells via a process called handover. Network users wish that the service provided to them is uninterrupted, whether with regard to the quality of phone calls or the speed with which they surf the Internet.

Self-Organizing Networks (SONs) is an evolving technology used to automate planning, configuration, optimization, and healing of networks. SON is included as part of the mobile networks standards such as such as Long Term Evolution (LTE). The quick evolution in wireless network industry have led to parallel operation of 2G, 3G, 4G, 5G, and emerging 6G networks that need to be managed and controlled with minimal human effort. SON is a promising technology to realize solutions for the control and management of this heterogeneous network regime. The technology suggests a set of concepts to automate network management toward a goal of improving quality of service (QoS) and reduce burdens of networks management on network administrators [1].

2.2.1 Operation Principle of Self-Organizing Networks

With SON, network administrators predefine a set of key performance indicators (KPIs) regarding QoS and other operational functions. Then, the network uses modules and algorithms to self-monitor and optimize its parameters, trying to achieve the predefined KPIs. This is considered as a closed loop control process, by which a network gains understanding of the operation environment and users' behavior and adapts its parameters accordingly to achieve the intended performance goal, but at same time avoid any misconfiguration of parameters that may lead to service disturbances [2]. In the following subsection, we elaborate more on the features of SONs illustrated in Figure 2.1.

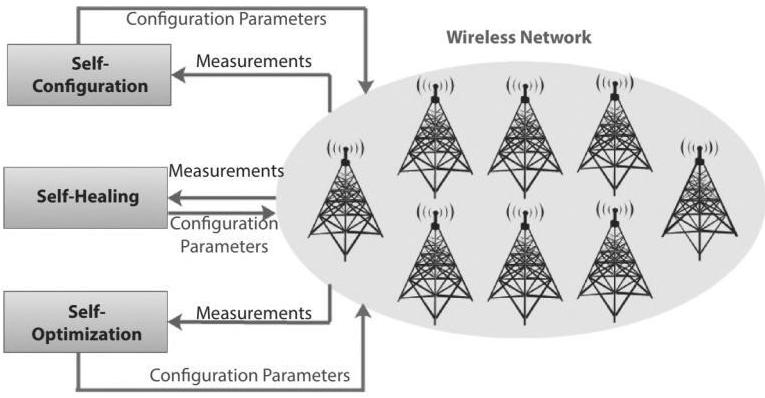


Figure 2.1 SON features.

2.2.2 Self-Configuration

Mobile communications networks are heterogeneous networks comprised of multiple technologies, such as LTE, EDGE, and UMTS. The number of mobile users is incredibly increasing which makes the installation and configuration of base stations a tedious process. Therefore, self-configuration is a process that reduces the time required for these tasks.

Self-configuration provides an initial setup of the network elements. It consists of three stages. The first stage relates to automatic connection to the network, security procedure, and establishing a secure connection between network elements and the network core. The second stage is the programming of network elements, while the third stage relates to the configuration of radio parameters.

2.2.3 Self-Optimization

Mobile networks are dynamic in nature. This pertains to traffic characteristics, the volume and variability of data exchanged between network elements, the joining of new users, the leave of others, and the movement of users among network cells. This results in variations of network performance as well as the level of service that users are experiencing. Therefore, self-optimization aims to maintain an optimal performance level for all network elements, through analysis of data measured and exchanged by network elements.

2.2.4 Self-Healing

The larger the network size, the more likely that failures will occur. The objective of self-healing is to continuously monitor the network in order to automatically detect and recover from unexpected possible failures. In future networks, it is expected that self-healing enables the network to predict faults and automatically take the necessary measures to avoid service degradation and disruptions.

2.2.5 Key Performance Indicators

KPIs are simple indicators that represent network performance. Here, we present examples of some important indicators:

- Channel Quality Indicator: This represents the connection quality to all users in a cell. Obstacles and multipath fading are major factors that impact channel quality.
- Handover Rate Indicator: This represents the mobility pattern of network users. It indicates the signaling traffic on the backbone network units which affects the overall network performance.
- Cell Load Indicator: This represents the amount of load on a cell, in terms of users, traffic load, or a cost function.
- Quality of Experience (QoE): This represents the satisfaction level of all users in the network or within each cell. Such indicator would characterize the QoS level users are experiencing.

2.2.6 SON Functions

It is important to discuss the fundamental optimization tasks of SONs. In this section, we present some important tasks:

- Coverage: Coverage optimization is a process through which a network tries to cover an intended area with minimal number of base stations and transmit power levels.
- Capacity: Capacity optimization refers to the process of providing users with the best possible QoS using minimal radio resources. This would imply radio frequency assignment and interference mitigation techniques.
- Mobility: Mobility optimization deals with the process of ensuring transparent user movement between cells and at the same time minimizing the number of unnecessary handover requests.
- Load Balancing: This refers to the process of distributing the load among network base stations, trying to maximize the QoE in the network and minimize the overhead on core network elements.

2.3 Cognitive Networks

Nowadays, communication networks are getting more complex and their configuration and management to achieve performance goals have become a challenging task. This is due to the following:

- The significant increase in the number of network users.
- The increase of the number of required networking elements at the network core.
- The huge number of mobile applications.
- The diversity of traffic.

The idea of cognitive networks is to improve the performance of networks and reduce the effort required for their configuration and management. Unlike current technologies, in which networking elements are unable to make intelligent decisions, the elements of a cognitive network have the ability to learn and dynamically self-adjust as response to changing channel and network conditions. Cognitive network elements utilize the principles of logic and learning in order to improve performance. Decisions are made to improve the overall network performance, rather than the performance of individual network elements. Thus, cognitive networks achieve the goal of intelligent, self-adjustment, and improved network performance, by intelligently finding optimal values of many adjustable parameters. They are required to learn the relationships among network parameters of the entire protocol stack.

As we indicated, a cognitive network should provide better performance to users. The cognition can be used to improve: utilization of network resources, QoS, security, access, control, or any other issue related to network management.

It must be emphasized that cognition is not only related to wireless networks, but also the idea applies to the management of network infrastructure and the various network elements [3]. To stimulate transition to cognitive networks, their performance must outweigh all additional complexities that they require. The question is how to measure the cost of a cognitive network. Such cost would primarily depend on the communications required to apply cognition, the architecture complexity, maintenance cost, and the operational complexity. For example, in wired networks, user's behavior is clear and easily predictable, and therefore, it may not be interesting for some people to employ cognition with this type of networks. On the contrary, wireless networks often include heterogeneous elements and have characteristics that cannot be easily predicted, making them the best candidates to adopt the cognition concept.

Cognitive networks should use different measures, tools, and patterns as inputs to the decision-making processes. Then, they come up with results in the form of procedures or commands that can be implemented in modifiable network elements. It is important to note that the cognitive network must adapt to changes in the environment in which it operates and anticipate problems before they occur. Their architecture must be flexible, scalable and be supportive of future improvements and extensions.

Several research studies have been discussing the architecture and functionalities of cognitive networks. There is a need to rethink about network intelligence from being dependent on resource management to understanding the needs of network users and then transferring intelligence also to the elements of the network.

The central mechanism of the cognitive network is the cognitive process. This process implements real learning and decides the appropriate responses and actions based on observations in the network. The operation of the cognitive process mainly depends on whether its implementation is central or distributive as well as on the amount of state network information.

2.4 Introduction to Machine Learning

ML is a subset of AI. The aim of ML is to develop algorithms that can learn from data and solve specific problems in some context as human do [4]. ML has been proving its ability

to overcome the challenges and complexities of mathematical formulation and solution of complex problems, including wired and wireless networking problems that require effective methods to quickly respond to dynamical changes of channels as well as the increasing diversification of services. Dynamic ML algorithms are able to process data and learn from it. They are replacement of complex algorithms which are written in a fixed way to conduct specific tasks.

The basic concept of ML is through training data that is used as input to the learning algorithm. The learning algorithm then produces a new set of rules, based on inferences from data, which results in a new algorithm. The new algorithm is officially referred to as the ML model. Traditional algorithms are comprised of a set of pre-programmed instructions used by the processor in the operation and management of a system. However, instructions of ML algorithms are formed based on real-life data acquired from the system environment. Thus, a machine is fed a large amount of data, it will analyze and classify data, then use the gained experience to improve its own algorithm and process data in a better way in the future. The strength of ML algorithms lies in their ability to infer new instructions or policies from data. The more data is available for the learning algorithms during the training phase, the more ML algorithms will be able to carry out their tasks efficiently and with greater accuracy.

2.4.1 ML Types

Depending on the type of tasks, there are two types of ML:

- Regression Learning
  It is also called prediction model, used when the output is a numerical value that cannot be enumerated. The algorithm is requested to predict continuous results. Error metrics are used to measure the quality of the model. Example metrics are Mean Absolute Error, Mean Squared Error, and Root Mean Squared Error.
- Classification Learning
  The algorithm is asked to classify samples. It is of two subtypes: binary classification models and multiple classification models. Accuracy is used to measure the quality of a model.

The main difference between the algorithms for classification and regression is the type of output variable. Methods with quantitative outcomes are called regressions or continuous variable predictions. Methods with qualitative outputs are called classifications or discrete variable predictions.

2.4.2 Components of ML Algorithms

A formal definition of a ML algorithm is "A Computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks T, as measured by P, improves with experience E" [5].

- Tasks: A task defines a way to process an object or data. An example task is classification, which is a process of assigning a class label to an input object

or data point. Regression is another task example, which involves assigning a real value to an object or data point.

- Performance Measure: Defines the criteria by which a ML algorithm is evaluated. In classification algorithms, accuracy refers to the percentage of correct assignment of class labels to objects or data points. Normally, data is divided into two sets. The first is used for training, while the second is used for testing.
- The Experience: It refers to the knowledge that a ML gains while learning. It divides the ML algorithms into the types explained in the next subsection.

2.4.3 How do Machines Learn?

Intelligent machines learn from the data available in their environment. The process of applying ML consists of two phases: The training phase and the decision-making phase. In the training phase, ML techniques are used to learn the system model using training dataset. In the decision-making phase, the machine shall be able to estimate the output for each input data point using the trained model.

According to the training method, ML techniques can be classified into four general types. Many advanced ML techniques are based on those general types. Figure 2.2 illustrates these types.

2.4.3.1 Supervised Learning

This learning method requires a supervisor that tells the system what is the expected output for each input. Then, the machine learns from this knowledge. Specifically, the learning algorithm is given labeled data and the corresponding output. The machine learns a function that maps a given input to an appropriate output. For example, if we provide the

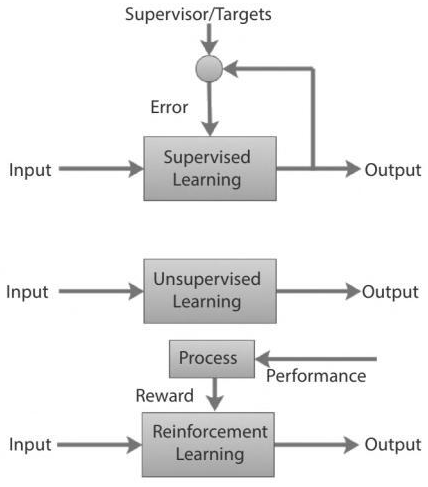


Figure 2.2 Machine learning types.

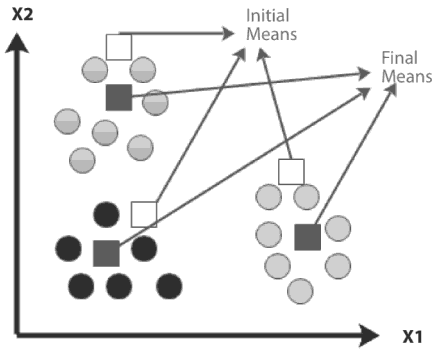


Figure 2.5 Illustration of K-means clustering.

- Density-Based Clustering: In this type of clustering, the algorithm tries to find the areas with high and low density of observations. Data points that are within a specified distance become centers of a cluster. Other data points either belong to a cluster border or considered as noise.

2.4.3.3 Semi-Supervised Learning

This learning approach combines both supervised and unsupervised ML techniques. Thus, the machine learns from both labeled and unlabeled data. This approach is more realistic for many applications, wherein small amount of labeled data is available, but the collection of large set of labeled data is not easy or impractical.

2.4.3.4 Reinforcement Learning

Similar to unsupervised learning in the sense that the machine has to learn by itself. However, a reward mechanism is applied to tune the algorithm based on observation of performance, enabling continuous self-update of the machine. Reinforcement learning algorithms try to define a model of the environment by determining the dynamics of the environment. The algorithm uses an agent which interacts with a dynamic environment in a trial-and-error manner. It provides feedback to the algorithm. The agent makes decisions on what actions to be performed to optimize the reward. A policy determines how the agent should behave at a given time. Thus, the algorithm learns by exploring the environment and exploiting the knowledge. The feedback from the environment is used to learn the best policy to optimize the cumulative reward.

The most commonly known reinforcement algorithm is the Q-Learning. The RL algorithm interacts with the environment to learn Q values. The Q value is initialized. The machine observes the current state, chooses an action from a set of possible actions, and performs the action. The algorithm observes the reward and the new state. The Q-value is updated based on the new state and the reward. Then, the state is set to the new state and the process repeats until a terminal state is reached.

2.4.4 ML and Wireless Networks

It is expected that future wireless networks will be highly integrated and a qualitative change will occur regarding the use of high frequencies and wide channels. In addition, the networks are expected to run a large number of base stations and serve high density of users. Future communication networks are dynamic and may also be without cells and massive-MIMO. They will be intelligent, flexible, and highly resilient [8]. ML is a promising tool for efficient management of future wireless networks.

2.5 Software-Defined Networks

Current networks are characterized by their distributed nature, as each node (router/switch) has the ability to view and act on the system partially and locally. Thus, global learning from network nodes that have a holistic view on the system will be very complicated. Further, current network designs impose significant limitations on network performance, especially under high traffic conditions. Consequently, the increasing demand for reliable, fast, scalable, and secure networks can adversely affect the performance of existing network devices due to the need to deliver a large volume of data both in the network infrastructure and devices. Current network devices lack the flexibility to handle different types of packets that may carry different contents due to the basic implementation of hard-wired routing rules. In addition, the networks that form the backbone of the Internet must be able to adapt to the changing conditions without needing much effort for hardware and software adjustments.

In order to reach a solution to the above discussed limitation issues, the rules for data processing must be implemented through software modules and not embedded in the hardware. This approach enables network administrators to have more control over the network traffic, and thus can greatly improve the network performance and effectively use the network resources. This innovative approach is called Software-Defined Network (SDN) [9].

SDN was released as open source software in 2008 with the OpenFlow project at Stanford University. It decouples the control and data planes in routers and switches, allowing the underlying infrastructure to be separated from application and network services. Thus, SDN separates the decision-making modules about where traffic is sent [the control plane (CP)] from the underlying systems responsible for forwarding the actual traffic (the data plane). Network resources are managed by a centralized controller which performs as the network operating system. The controller can dynamically program the network in real time. It collects information about network status and operation details. Therefore, the controller can globally detect available network resources and requirements. This paradigm creates a global view of the entire network, enabling global automatic management and control without needing to configure devices individually. The SND technology has several advantages:

- Efficient utilization of network resources.
- Enables development of programming-based solutions for network configuration and management.
- Provides a perfect ecosystem for ML paradigm and intelligent applications.

- Simple and improved network management, control, and data manipulation, since network administrators can remotely alter the network configuration and operation as response to dynamical changes in the network.
- High speed, through optimal handling of the traffic load.
- Adopts the virtualization technology, which allows running multiple applications over the same shared hardware.

Combining AI and SDN has been attracting researchers in recent years to develop network management and operation mechanisms. The SND architecture provides centralized control of network policies and enables administrators to effectively overcome problems with ML methods.

2.5.1 SDN Architecture

The architecture of SDN is comprised of three planes:

- Data Plane: comprised of the forwarding devices, i.e., switches and virtual switches. Unlike distributed network architectures, in which switching and routing devices listen to events from neighboring network elements and make decisions based on a local view, switches and routers are responsible for forwarding, dropping and modifying packets based on policies received from the CP.
- Control Plane: The CP is considered to be the brain of SDN. It can program network resources and dynamically update the rules of forwarding, in addition to making the management of the network flexible through the centralized controller. The centralized controller controls communication between switches and applications. On the other hand, the controller exposes the network status and summarizes the information to the application plane. Also, the CP translates the requirements from applications to specific policies and distributes them to devices. Further, it provides the basic functions needed by most network applications such as routing algorithms, network topology, device configuration, and state information notifications.
- Application Plane: composed of network applications that define management and optimization policies to be applied on the network. Applications can get network state information from the controller and implement the needed control to change network behavior.

The inclusion of ML in SDN may require a new architectural structure that differs from the traditional of SDN. In [10], a new plane is proposed called the knowledge plane KP as shown in Figure 2.6. The KP hosts ML algorithms that use statistical learning to learn the network behavior. These algorithms contribute to decision-making. Hence, the KP in SDN communicates directly with the controller, which, in turn, asks the network elements to implement decisions.

The controller gets information from network devices through the OpenFlow protocol. A server is used to process information and run ML algorithms. The execution of recommended commands is the responsibility of the controller which is connected to the KP. On the top, the application plane is running to manage the network.

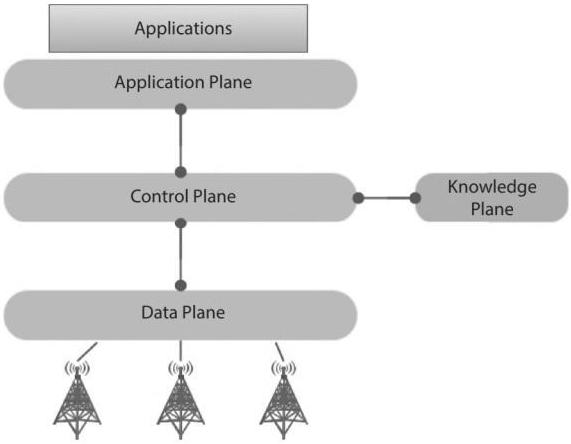


Figure 2.6 The SDN architecture with knowledge plane.

2.5.2 The OpenFlow Protocol

The open source OpenFlow protocol enables the realization of the SDN technology. It has been used for researching different protocol designs over existing hardware. OpenFlow is widely used for the communication between the control and the data planes. It is developed by the Open Networking Foundation (ONF). It is the interface between devices and the SDN controller, providing the rules for switching control features from network devices to the central controllable software. It has a controller and a switch, functioning as secure channel as shown in Figure 2.7. The controller can modify, discard, and send packets to the switch. The path of the packet is determined at the times of packet transmission. OpenFlow calculates the path and sends it to the switch, which stores it in the Flow Table. When a switch receives a packet, it looks up the flow table and sends it along the stored path [11]. The primary task of the switch is to exchange data using flow tables, which are controlled by

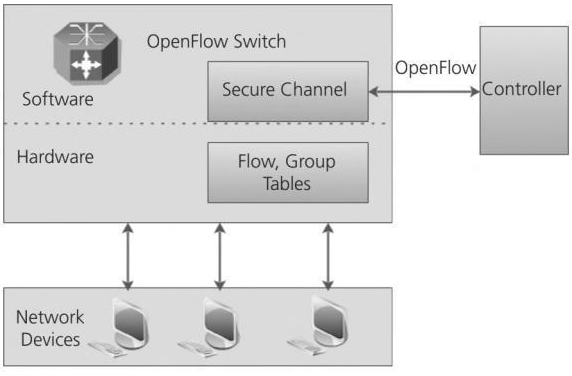


Figure 2.7 The OpenFlow architecture.

the controller of the CP. This architecture simplifies the design of switches and reduces their tasks, because they have become just data deliverers, without being required to perform any of the control functions.

The implementation of an SDN controller can be centralized or distributed. In the centralized implementation, a single SDN controller centrally controls and manages all network devices, which would possibly lead to bottleneck. Distributed implementation of the SDN controller would overcome this issue. The CP may include multiple controllers, depending on the network size. This will help boosting the network performance.

2.5.3 SDN and ML

SDN has strengthened applying programmatic principles on network, allowing network administrators to have precise, flexible, and innovative control of the network and thus reducing operational expenses.

The SDN architecture provides an opportunity to more efficient application of cognitive network concepts in a centralized system, leading to self-aware networks. The adoption of SDN-based systems highly depends on their success in providing solutions to problems that could not be solved by traditional network architectures and protocols [12].

Applying ML techniques with SDN is considered to be effective for the following reasons [13]:

- The recent advanced developments in computing and the accompanying advanced processors, thus creating a new opportunity to apply promising learning techniques.
- It is well known that ML algorithms depend on data. The SDN controller has a holistic view on the network and is able to collect different network data, simplifying the application of ML algorithms.
- Based on the ability of the SDN to act in real time and deal with historical data, ML techniques can create intelligence in the controller unit, by conducting data analysis relying on analyzed data in decision-making and thus improving the network and its services.
- The programmatically feature of SDN can help to find optimal solutions to network problems such as configuration and resource allocation. Thus, ML algorithms can be implemented in real time.

2.6 Cognitive Radio Networks

The Federal Communications Commission (FCC) defines cognitive radio as: "a radio that can change its transmitter parameters based on interaction with the environment in which it operates".

The main features of cognitive radio are as follows [14]:

- Awareness: CR is aware of its surrounding environment through the sensing capability.

that are able to optimize and configure themselves. We focus on recent published research and try to shed light on important research aspects of the present and future. Our goal is to assist readers to identify the scientific areas and specific issues that need further research and exploration. We divide the discussion into three parts. In the first part, we focus on Cellular networks, while the second part focuses on wireless local area networks (WLANs). The third part is devoted to cognitive radio networks.

2.7.1 Cellular Networks

2.7.1.1 Energy Saving

With the steady increase in the number of users of wireless networks and the need to deploy large number of base stations, and since base stations consume large energy; operating the network with minimum energy is a challenge. One way to reduce energy consumption is the idea of turning off some base stations if users can be served from others, while maintaining a reasonable QoS level. Learning the operation of the network over time helps in improving decisions about which base stations might be switched off.

An SDN-based ML system for energy saving is proposed in [15]. Performance of neural networks and SVM algorithms is compared. The network trains itself using data collected from base stations and recommends the operator time periods during which some base stations are predicted to handle very low traffic and therefore can be switched off.

The authors of [16] propose a Q learning method for base station on-off switching. The switching of base stations is defined as the actions, while the traffic load is defined as the state. The overall objective is to minimize energy consumption. Policy values are used by the controller to decide on switching. After performing a switch operation, the system state is changed and the energy cost of the former state is computed. If the energy cost of the newly executed action is smaller than energy costs with other actions, then the controller updates the policy value in order to increase the probability of selecting this action. With time, the optimal switching mechanism is obtained.

2.7.1.2 Channel Access and Assignment

The effective use of wireless channels has become an urgent necessity, as many heterogeneous systems operate in the same frequency band. Thus, coexistence and organized access of the shared frequency chunks by systems are necessary. Consequently, any design of the wireless channel sharing mechanism should be based on a prediction of the behavior of networks users.

In [17], the authors propose deep reinforcement ML-based MAC protocol for the coexistence of multiple heterogeneous networks. The method allows time-sharing access of the spectrum, by a series of observations and actions. The MAC protocol does not have to know the MAC mechanism of other networks and tries to maximize the throughput of all coexisting networks. The authors of [18] employ reinforcement learning for managing cell outage and compensation. The system state is constituted by the allocation of users to the resources of cells and the channel. Actions are related to the power control, while the rewards are quantified in terms of SINR improvement. The authors show that such ML-based approach provides improved performance.

In [19] and [20], the authors use clustering algorithms to group users that share common interests to reduce interference and collisions. The authors show that such clustering improves the access opportunities for wireless users. A cluster header (CH) is selected to collect data from all devices. It sends the data to base stations which schedule the transmission.

Channel assignment is a well-known challenging issue in wireless networks, especially with systems of limited channels. Such systems highly suffer from interference, and the optimal selection of channels becomes important. Channel assignment problems are normally formulated as convex optimization problems, where algorithms needed to solve such problems are computationally complex. In a dynamic environment of wireless networks, understanding the behavior of network users and learning from previous data is expected to be a good approach for improving channel assignment mechanisms.

The paper of [21] uses ML approach to tackle the channel assignment problem and developed a computationally efficient solution for this problem. The objective is to maximize the total data rate experienced by all users assuming limited resources and large number of network users. The convex optimization problem is converted to a regression problem. Ensemble learning is utilized to combine different machine learning models and improve the prediction performance.

2.7.1.3 User Association and Load Balancing

User association and load balancing is a challenge that has been attracting researchers of wireless networks. The question is how to optimally assign users to base stations and distribute the load in a balanced way among network base stations. The aim is to achieve high QoS to all users and at the same time efficiently utilize network resources.

The authors of [22] investigated the use of deep learning to perform user-cell association to maximize the total data rate in massive multiple input multiple output (MIMO) networks. The authors show how a deep neural network; that gets the geographical positions of users as input; can be trained to approach optimal association rule with low computational complexity. Association rule is updated in real-time considering mobility pattern of network users.

A method for cell outage detection was proposed in [23] using neural networks and unsupervised learning. The main feature of the method is the training of the network which can be performed in advance even when the cell outage data is not available. Moreover, the developed method could work in time-varying wireless environments. The machine learns from measurement reports of signal power which are collected by mobile devices.

The research work in [24] proposes a distributed, user-centric ML-based association scheme. The algorithm is based on fuzzy Q-learning, where each cell tries to maximize its throughput under infrastructure capacity and QoE constraints. With this scheme, cells broadcast data values to guide users to associate with best cells. The values reflect the possibility of a cell to satisfy a throughput performance level. Each cell tries to learn the optimal values through iterative interaction with the environment. In [25], the authors used realistic mobile network data and investigated methods for failure prediction. They compared the performance of the SVM and several neural networks.

2.7.1.4 Traffic Engineering

The process of analyzing traffic in networks is normally performed through examining messages and extracting information from them. This helps in developing effective assessment strategy of how network users behave and identifying their goals from using networks, as well as knowing the data paths and communication patterns. All of this can be used to provide information for network management algorithms and to optimize the use of network resources.

Traffic engineering is related to two processes: Prediction and Classification. Traffic prediction is a process for anticipating the traffic volume based on previously observed traffic volume; while traffic classification is a process of identifying the type of traffic. The process of traffic classification is based on collecting large number of traffic flows and analyzing those using ML techniques. Classifying traffic would help in improving security, QoS, capacity planning, and service differentiation. Classes could be: HTTP, FTP, WWW, DNS, P2P, Skype, and YouTube. Classification can be based on one or more traffic parameters, such as port number, packet payload, host behavior, or flow features [26].

ML is considered as an efficient tool in [27] for applying traffic engineering concepts. The authors use naïve Bayes classification, which uses supervised learning to construct a learning model for traffic analysis and classification. They developed a new weight-based kernel bandwidth selection algorithm to improve the constructed kernel probability density and ML model. The authors of [28] developed and SDN-based intelligent streaming architecture which exploits the power of time series forecasting for identifying users' data rate levels in wireless networks, trying to improve the QoS of delivering video traffic. The SDN architecture is comprised of Data Plane (Switching devices), QoE management plane (management, bandwidth estimator, monitor, policy enforcer, and bandwidth forecaster), and CP aims to support the delivery of video services and to provide the QoE-based resource allocation per user.

The paper of [29] compares the performance of several supervised and unsupervised ML algorithms to classify traffic as normal or abnormal. In [30], the authors propose a traffic classification algorithm based on flow analysis. The algorithm is designed for SDN platforms.

The work in [31] uses traffic classification as part of a traffic scheduling solution for a data center network managed by SDN. ML techniques are used to classify elephant traffic flows, which require high bandwidth. Then, the SDN controller uses classification results and implements optimization of traffic scheduling. The authors of [32] use two phases for detection of elephant flows using ML techniques in SDN-based networks. In the first phase, packet headers are used to distinguish between elephant flows from mice flows, low bandwidth flows. A decision tree ML algorithm is then used to detect and classify traffic flows. Also, the authors of [33] developed an OpenFlow-based SDN system for enterprise networks. Several classification algorithms were compared.

An application of ML for improving the quality and latency of real time video streaming is proposed in [34]. The video quality is achieved through rate control, employing a DL-based adaptive rate control scheme. Two RL models are used. The first one is for prediction of video quality model, while the second is video quality RL. The predictor uses previous video frames to predict quality of future frames. The RL algorithm adopts and

trains the neural network based on historic network status and video quality predictions to decide rate control actions.

In their research published in [35], the authors developed a method for traffic prediction based on the SDN architecture, where the controller gathers data and uses it to classify data flows into categories. Neural network algorithm is used to predict the expected traffic, leading to a system that can act to avoid traffic imbalance before it occurs.

2.7.1.5 QoS/QoE Prediction

QoS parameters are normally used by network administrators to assess the network performance. The parameters include throughput, loss rate, delay, and jitter. However, QoE is a parameter used to represent the user perception and satisfaction of the services. Developing prediction methods for QoS and QoE parameters helps network operators and service providers to offer high quality services [13]. SDN has been used to facilitate the implementation of different algorithms for QoS/QoE prediction [36–39].

The authors of [36] propose a linear regression ML algorithm for QoS prediction in SDN-based networks. A decision tree approach is used to detect relations between KPIs and QoS parameters. The authors show that the method can predict congestion and thus provide recommendations on QoS improvement. The researchers in [37] utilize two ML techniques for estimating QoS parameters for video on demand applications.

QoE prediction was addressed in [38–39]. The method of [38] was designed for video streaming in an SDN-based network, where QoS parameters are employed to estimate the mean opinion score. The SDN controller is used to adjust video parameters to improve QoE. In [39], the authors use neural network and KNN algorithms for predicting QoE parameters using video quality parameters.

2.7.1.6 Security

Users only use secure networks. One major issue in networking is the attacks by intrusions. Detecting intrusion and responding to attacks is a real challenge, especially in wireless networks where data is communicated over a shared media. With the advent of ML technology, researchers have been trying to exploit ML techniques to overcome this problem. ML methods can process and classify traffic flows based on observable properties such as number of packets in a flow, flow duration, packet size, inter-packet arrival time, and flow size in bytes. Based on these properties, more advanced features can be computed.

The authors of [40] propose a system for ML-based flow classification integrated in SDN. It exploits methods of extracting knowledge that can be used by the controller in order to classify flows. A supervised ML algorithm has been used for identifying the underlying application flow, while unsupervised learning algorithm has been used for clustering flows in order to identify unknown applications. The system is also able to detect groups of related flows and proved to detect anomaly and botnet, as well as honeypot traffic rerouting.

The authors of [41, 42] show that employing user centric approaches combined with ML can improve the performance of anomaly detection in cellular networks. User centric approaches focus on the end user while developing designs and strategies for networks, thus the need of end users will tailor networking solutions. The study uses the SVM, KNN,

and an optimized version of decision tree, wherein algorithms learn and predict QoE scores for users. A node is judged to be dysfunctional if the maximum number of users connected to this network node have poor QoE scores.

In [11], the authors developed an SDN-based system for real time intrusion detection using a deep learning-based approach. Data sets are used to train the ML algorithm, following the supervised learning approach. Then, a flow inspection module examines the flows and decides whether it is an intrusion flow or not. The SDN paradigm facilitates the implementation of the proposed method, as it provides means for designing flow-based monitoring and control mechanisms.

A detailed intelligent system for an automated control of large-scale networks is developed in [43]. The system architecture exploits SDN and deep RL methods for intelligent network control. Among other objectives, the system can serve applications that require traffic analysis and classification. RL involves processes that learn to make better decisions from experiences by interacting with all network elements. The SDN architecture is comprised of three planes: forwarding plane, the CP, and the AI plane. The function of the forwarding plane is forwarding, processing, and monitoring of data packets. The CP connects the AI plane and the forwarding plane. The SDN controller manages the network through standard southbound protocols and interacts with the AI plane through the northbound interface. The AI plane generates policies. It learns the policy through interaction with the network environment. An AI agent processes the network state data collected by the forwarding plane, then transfers the data to a policy through RL that is used to make decisions and optimization.

The researchers in [44] use KNN classification algorithm for detecting several types of attacks. The authors pointed out that with large training dataset, the computation of distances between the test point and training data is time-consuming as the algorithm needs also to sort and find the closest K neighbors. Author in [45] uses unsupervised ML for detecting anomalies in real networks. The proposed approach enables anticipation of anomalies before they become a real problem.

The paper of [46] provides a detailed review of recent studies that combines ML and SDN technology to solve the intrusion detection problem. The authors compare the performance of supervised, unsupervised, semi-supervised, and DL algorithms.

2.7.2 Wireless Local Area Networks

In recent years, we see tremendous widespread of WLANs, as they evolve to meet user's requirements, especially the high speed Internet connection. Accurate prediction of WLANs performance is important for managing network resources. However, due to interference and the interactions between the physical and data link layers as well as the heterogeneity of WLAN devices, predicting and estimating the performance of WLANs is a difficult task. Many of the solutions use the Signal-to-Noise and Interference Ratio (SNIR) parameter. However, it has been proven that relying on this parameter to estimate the performance does not lead to satisfactory results. In fact, the performance of WLANs is more complex to be measured using SNIR, and it is a function of large number of interacting and related parameters that may change over time.

A plethora of research studies has developed various solutions to different challenges based on the traditional architecture of WLANS, aiming to optimally exploit network

2.7.2.3 Channel Allocation and Channel Bonding

Even with centralized control, optimal channel allocation problem in WLANs is difficult to be solved in an acceptable complexity level. Recently, researchers have been trying to leverage ML methods to find solutions in feasible time.

In [61], the authors propose a ML method for assigning channels to WLANs APs. The method is based on passive monitoring of data in each cell. Using ML, it calculates the performance loss due to interfering users and finds the best channels for the cells that minimize interference. The algorithm minimizes airtime usage of interfering links in neighboring cells. Due to the dynamic nature of WLANs, the process is repeated iteratively. The authors of [62] concluded that a central control of APs is needed even if the network is influenced by neighboring unmanaged APs. Their approach results in a self-organizing system for channel allocation in WLANs based on cooperation between APs. The authors show that the proposed system leads to a stable network of high performance.

In [63], the authors use ML techniques to learn implicit performance models from real-world measurements. The techniques do not need to know the details of interacting parameters. The authors used the developed model for channel allocation and power control.

2.7.2.4 Latency Estimation and Frame Length Selection

Latency is a key factor that impacts the performance of modern mobile applications. In [64], the authors found that, latency depends on three main parameters: Channel utilization, the number of online devices, and the SNR. WiFi latency can be modeled using these related factors. The authors developed and compared the performance of supervised ML-based algorithms used to measure, characterize, and predict delay in large-scale WLANs. Training is implemented using data sets obtained from field measurements.

Selecting a proper frame length is an important issue in WLANs, where it impacts the performance and users' QoE in the network. The selection problem requires advanced techniques able to utilize information on practical settings in real-time.

The work in [65] proposes an SDN-based solution for frame length selection in WLANs. The system proposes inclusion of ML techniques in SD-WLANs to optimize the selection of frame length for each user based on channel conditions as well as overall performance indicators. The supervised learning approach is used, where the algorithm is deployed on the management plane of the SDN architecture. The CP periodically feeds the algorithm with network knowledge about channel conditions and users' state.

The research work of [66] proposes a ML-based approach for the implementation of QoS management model in wireless networks. The ML system uses both supervised and unsupervised algorithms to identify key quality indicators for network users which represent an estimation of the quality as perceived by users considering influencing factors. Also, the ML concept is used for providing information about areas where corrective actions are required.

2.7.2.5 Handover

Transparent handover with minimum overhead is still an open issue in WLANs. Though the 802.11r standard developed protocols that help implementing seamless handover between

WLAN cells, still APs and users need to be highly engaged in the handover process. This impacts the performance of APs, especially in dense deployments; wherein handover rate is expected to be high. With the advancement in AI and ML; coupled with the evolving SDN technology, researchers are trying to develop methods that allow low cost and successful transparent mobility among WLAN cells.

An example effort is published in [67], where the authors developed an SDN-based solution for controlling and managing handover in WLANs. The proposed solution allows the devices to seamlessly move across cells without losing the QoS level.

The researchers in [68] developed a framework to optimize the handover process and balance the network throughput and handover rate. Unsupervised ML algorithm is used to classify users according to their mobility patterns. Then, deep RL is used to optimize the handover process in each cluster. The received signal power by the user from APs is used as the state vector. The reward is considered to be the weighted sum between the handover rate and the throughput.

In [67], the authors developed and tested an SDN-based solution for providing seamless handover in WLANs based on virtual APs. The solution maintains QoS requirements of real time applications in terms of packet loss and delay.

2.7.3 Cognitive Radio Networks

Currently, ML-based spectrum sensing techniques are proposed. The existence of PUs is determined through two phases. In the first, signal features are extracted employing one of the spectrum sensing methods. In the second phase, decisions are made about PUs' activity by applying ML algorithms. The authors of [68] used the energy detection approach to extract signal features which were used to train the K-mean-based ML model, whereas [69] proposes a probability vector as features of ML method. Probability vector has shown superior performance, whereby it alleviates the dimension of the feature vector and, hence, reduces the time duration of the ML model. In [70], the authors propose to use the eigenvalues/eigenvector as features, whereby these features are derived from constructing covariance matrix samples from different SUs' signals. The authors of [71] derived the eigenvalues/eigenvector features by applying principle component analysis of the signal samples. Based on information geometry theory and application, the work in [72] innovate novel features by measuring the distance between two probability distributions on a statistical manifold. The research efforts in [73–76] focus on finding the circularly characteristics that help in differentiating between the transmitted and noise signals. In their models published in [77, 78], the authors study the case where SUs catch more than one PU signals, whereas [79] investigated the mobility issue of CR systems.

References

1. Gacanin, H. and Ligata, A., Wi-fi self-organizing networks: Challenges and use cases. *IEEE Commun. Mag.*, IEEE, 55, 7, 158–164, 2017.
2. Lohmüller, S., Cognitive Self-Organizing Network Management for Automated Configuration of Self-Optimization SON, in: *PhD. Dissertation*, University of Augsburg, 2019.

3. Thomas, R., DaSilva, L., MacKenzie, A., Cognitive Networks (book chapter), in: *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*, Springer, Germany, 2007.
4. Thang, V.V. and Pashchenko, F.F., Multistage System-Based Machine Learning Techniques for Intrusion Detection in WiFi Network. *J. Comput. Networks and Commun.*, vol. 2019, Article ID 4708201, 13 pages, 2019. https://doi.org/10.1155/2019/4708201.
5. Mitchell, T., *Machine Learning, McGraw Hill series in computer science*, Mc- Graw-Hill, USA, 1997.
6. Liu, Y., Bi, S., Shi, Z., Hanzo, L., When Machine Learning Meets Big: A Wireless Communication Perspective. *IEEE Veh. Technol. Mag.*, IEEE, 15, 63–72, 2020.
7. Kaufman, L. and Rousseeuw, P., *Finding Groups in Data: An Introduction to Cluster Analysis*, JohnWiley & Sons, US, 2018.
8. Andrews, J., Buzzi, S., Choi, W., Hanly, S., Lozano, A., Soong, A., Zhang, J., What will 5G be? *IEEE J. Sel. Areas Commun.*, 32, 1065–1082, 2014. IEEE.
9. Agarwal, S., Kodialam, M., Lakshman, T., Traffic engineering in software defined networks. *Proc. IEEE INFOCOM*, pp. 2211–2219, 2013.
10. Mestres, A., Rodriguez-Natal, A., Carner, J., Barlet-Ros, P., Alarcón, E., Solé, M., Muntés-Mulero, V., Meyer, D., Barkai, S., Hibbett, M., Knowledge defined networking. *ACM SIGCOMM Computer Communication Review*, vol. 47, pp. 2–10, 2017.
11. Lim, S., Software Defined Network Detection System. *Int. J. Recent Technol. Eng. (IJRTE)*, 8, 1391–1395, 2019.
12. Lin, P., Bi, J., Wolff, S., A west-east bridge based SDN inter-domain testbed. *IEEE Commun. Mag.*, 53, 2, 190–197, 2015.
13. Xie, J., Yu, F., Huang, T., Xie, R., Liu, J., Wangz, C., Liu, Y., A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges. *IEEE Commun. Surv. Tutorials*, 21, 393–430, 2019.
14. Elkhodr, M., Hassan, Q., Shahrestani, S., *Networks of the Future: Architectures, Technologies, and Implementations*, CRC Press Taylor & Francis Group, USA, 2018.
15. Kosmidesa, P., Adamopouloua, E., Demestichasa, K., Anagnostoua, M., Rouskasb, A., On Intelligent Base Station Activation for Next Generation Wireless Networks. *The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks*, Elsevier, 2015.
16. Li, R., Zhao, Z., Chen, X., Zhang, H., Energy saving through a learning framework in greener cellular radio access networks. *Proceedings of GLOBECOM*, 1556–1561, 2012.
17. Yu, Y., Wang, T., Liew, S., Deep-Reinforcement Learning Multiple Access for Heterogeneous Wireless Networks. *IEEE International Conference on Communications (ICC)*, IEEE, 2018.
18. Onireti, O., A Cell Outage Management Framework for Dense Heterogeneous Networks. *IEEE Trans. Veh. Technol.*, 65, 2097–2113, 2016.
19. Mohammadi, M. and Al-Fuqaha, A., Enabling Cognitive Smart Cities Using Big Data and Machine Learning: Approaches and Challenges. *IEEE Commun. Mag.*, 56, 94–101, 2018.
20. He, Y., Software-Defined Networks with Mobile Edge Computing and Caching for Smart Cities: A Big Data Deep Reinforcement Learning Approach. *IEEE Commun. Mag.*, 55, 31–37, 2017.

21. Jia, G., Yang, Z., Lam, H., Shi, J., Shikh-Bahaei, M., Channel assignment in uplink wireless communication using machine learning approach. *arXiv preprint arXiv*, 2001, 03952, 2020.
22. Zappone, A., Sanguinetti, L., Debbah, M., User association and load balancing for massive MIMO through deep learning. *Proceedings of IEEE Asilomar Conference on Signals, Systems, and Computers*, pp. 1262–1266, 2018.
23. Lin, P., Large-Scale and High-Dimensional Cell Outage Detection in 5G Self-Organizing Networks. *Proceedings of APSIPA Annual Summit and Conference*, pp. 8–12, 2019.
24. Pervez, F., Jaber, M., Qadir, J., Younis, S., Imran, M., Fuzzy Q-learning-based user-centric backhaul-aware user cell association scheme. *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC),* pp. 1840–1845, 2017.
25. Kumar, Y., Farooq, H., Imran, A., Fault Prediction and Reliability Analysis in a Real Cellular Network. *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1090–1095, 2017.
26. Boutaba, R., Salahuddin, M., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., Caicedo, O., A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. *J. Internet Serv. Appl.*, Springer, 9, 16, 2018. https://doi.org/10.1186/s13174-018-0087-2
27. Song, R. and Willink, T., Machine Learning-Based Traffic Classification of Wireless Traffic. *International Conference on Military Communications and Information Systems (ICMCIS)*, 2019.
28. Al-Issax, A., Bentaleb, A., Barakabitzex, A., Zinnery, T., Ghita, B., Bandwidth Prediction Schemes for Defining Bitrate Levels in SDN-enabled Adaptive Streaming. *15th International Conference on Network and Service Management (CNSM)*, 2019.
29. Fan, Z. and Liu, R., Investigation of machine learning based network traffic classification. *Proceedings of ISWCS*, pp. 1–6, 2017.
30. Song, C., Park, Y., Golani, K., Kim, Y., Bhatt, K., Goswami, K., Machine-learning based threat-aware system in software defined networks. *Proceedings of IEEE ICCCN*, pp. 1–9, 2017.
31. Glick, M. and Rastegarfar, H., Scheduling and control in hybrid data centers. *Proceedings IEEE PHOSST'17*, pp. 115–116, 2017.
32. Xiao, P., Qu, W., Qi, H., Xu, Y., Li, Z., An efficient elephant flow detection with cost-sensitive in SDN. *2015 1st International Conference on Industrial Networks and Intelligent Systems (INISCom)*, pp. 24–28, 2015.
33. Amaral, P., Dinis, J., Pinto, P., Bernardo, L., Tavares, J., Mamede, H., Machine learning in software defined networks: Data collection and traffic classification. *Proceedings of IEEE ICNP'16*, pp. 1–5, 2016.
34. Huang, T., Zhang, R., Zhou, C., Sun, L., QARC: video quality aware rate control for real-time video streaming based on deep reinforcement learning. *ACM Multimedia Conference*, ACM, 2018.
35. Azzouni, A. and Pujolle, G., Neutm: A neural network-based framework for traffic matrix prediction in SDN. *IEEE/IFIP Network Operations and Management Symposium*, 2018.

36. Jain, S., Khandelwal, M., Katkar, A., Nygate, J., Applying big data technologies to manage QoS in an SDN. *Proceedings of IEEE CNSM'16*, pp. 302–306, 2016.
37. Pasquini, R. and Stadler, R., Learning end-to-end application QoS from OpenFlow switch statistics. *Proceedings of IEEE NETSOFT'17*, pp. 1–9, 2017.
38. Letaifa, A., Adaptive QoE monitoring architecture in SDN networks: Video streaming services case. *Proceedings of IEEE IWCMC'17*, pp. 1383–1388, 2017.
39. Abar, T., Letaifa, A., Asmi, S., Machine learning based QoE prediction in SDN networks. *Proceedings of IEEE IWCMC'17*, pp. 1395–1400, 2017.
40. Comaneci, D. and Dobre, C., Securing Networks using SDN and Machine Learning. *IEEE International Conference on Computational Science and Engineering*, 2018.
41. Murudkar, C.V. and Gitlin, R.D., QoE-driven Anomaly Detection in Self Organizing Mobile Networks using Machine Learning. *2019 Wireless Telecommunications Symposium (WTS)*, pp. 1–5, April 2019.
42. Murudkar, C. and Gitlin, R., Machine Learning for QoE Prediction and Anomaly Detection in Self-Organizing Mobile Networking Systems. *Int. J. Wireless Mobile Networks (IJWMN)*, 11, 2, April 2019.
43. Yao, H., Mai, T., Xu, X., Zhang, P., Li, M., Liu, Y., NetworkAI: An Intelligent Network Architecture for Self-Learning Control Strategies in Software Defined Networks. *IEEE Internet Things J.*, 5, 4319–4327, 2018.
44. Zhu, L., Tang, X., Shen, M., Du, X., Guizani, M., Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks. *IEEE J. Sel. Areas Commun.*, 36, 628–643, 2018.
45. Côté, D., Using machine learning in communication networks. *J. Opt. Commun. Networks*, 10, D100–D109, 2018.
46. Sultana, N., Chilamkurti, N., Peng, W., Alhadad, R., Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-Peer Network Appl.*, 12, 2, 493–501, 2019.
47. Moura, H., Alves, A., Borges, J., Macedo, D., Vieira, M., Ethanol: A Software-Defined Wireless Networking architecture for IEEE 802.11 networks. *Comput. Commun.*, Elsevier, 149, 176–188, 2020.
48. Lei, T., Wen, X., Lu, Z., Li, Y., A semi-matching based load balancing scheme for dense IEEE 802.11 WLANs. *IEEE Access*, 5, 15332–15339, 2017.
49. Peng, M., He, G., Wang, L., Kai, C., AP Selection Scheme Based on Achievable Throughputs in SDN-Enabled WLANs. *IEEE Access*, IEEE, 7, 4763–4772, 2019.
50. Fulara, H., Singh, G., Jaisinghani, D., Maity, M., Chakraborty, T., Naik, V., Use of machine learning to detect causes of unnecessary active scanning in wifi networks. *Proceedings of WoWMoM*, pp. 1–9, 2019.
51. Ernst, J., Kremer, S., Rodrigues, J., A utility based access point selection method for IEEE 802.11 wireless networks with enhanced quality of experience. *Proceedings of IEEE ICC*, pp. 2363–2368, 2014.
52. Chen, J., Liu, B., Zhou, H., Yu, Q., Gui, L., Shen, X., QoS-driven efficient client association in high-density software-defined WLAN. *IEEE Trans. Veh. Technol.*, 66, 7372–7383, 2017.
53. Quer, G., Baldo, N., Zorzi, M., Cognitive call admission control for voip over ieee 802.11 using bayesian networks. *In Proceedings of GLOBECOM*, IEEE, pp. 1–6, 2011.

3

An Overview on Internet of Things (IoT) Segments and Technologies

Amarjit Singh

Jalandhar, Punjab, India

Abstract

The concept of IoT refers to the Internet of Things that can involve internet activity. But this can be done using the internetworking concept and aim to data information transfer. In other words, IoT can process for sharing information between virtual and system interaction. Using the IoT, it fetches the information using the sensors and other objects [1]. As one can with little of a stretch imagine, any certified duty to the improvement of the IoT ought to result from synergetic activities drove in different fields of data, for instance, communicate correspondences, informatics, contraptions, and human science. In such a capricious circumstance, it organizes this investigation to the people who need to advance toward this baffling train and add to its unforeseen development. It represents original dreams of this IoT perspective for enabling advances tested. What rises is that despite everything, significant issues will be confronted. This research paper includes the understanding of IoT and its different approaches.

***Keywords*:** IoT, networking, sensors, wireless communication, sensor networks

3.1 Introduction

Internet of Things (IoT) could be characterized assortment that is the internet; it is characterized as systems of systems that can associate millions of clients with a few typical internet conventions [2]. In IoT, the urban areas can be constructed where it manages with the parking spots, lighting, water system offices, commotion, and burn through, which can be checked continuously applications. We can fabricate keen homes that are extremely sheltered and progressively proficient to live. We can fabricate savvy conditions that can naturally be checking the contamination from air and water and empowering the early recognition of Tsunami, tremors, backwoods fires, and many annihilating debacles in the earth. A few modern, normalization, and study bodies engaged with the action of the development of answers to mollify the featured innovative prerequisites. This overview gives an image of the present cutting edge on the IoT [3]. IoT assumed expresses to a combine of extra problems about the framework's body outlooks. Low resources will depict the things

Email: amarjit.rhce@gmail.com

Pardeep Kumar, Vishal Jain and Vasaki Ponnusamy (eds.) The Smart Cyber Ecosystem for Sustainable Development, (57–68) © 2021 Scrivener Publishing LLC

framing the IoT to the amount of together estimation and essential limit. The future progressions of action need to give outstanding assumed to affirm adequacy additional than the understandable adaptability issues (Figures 3.1 and 3.2).

The IoT area prompts the universe of innovation and correspondence to another period where items can impart, register, and change the data according to the prerequisites. The IoT is a modification in outlook in the IT sector [4]. As from definition, the internet is the PC that organizes all-inclusive interconnected and uses the standard convention for serving the millions of clients everywhere the world. The guideline nature of the IoT, however, is the high impact; it will have on a couple of parts of normal day-by-day presence and lead of possible customers. From a private customer, the clearest impacts of the IoT would be perceptible in together the occupied and private arenas. Devilfish lived, e-prosperity, improved learning is only two possible application circumstances in which the new perspective will expect the significant activity in a matter of seconds. So, likewise, from business customers, the clearest outcomes will be comparably perceptible in fields, for example, motorization and present-day, co-appointments, business/process of the officials, and brilliant conveyance of people and items [5].

IoT develops quickly; it will be proceeding with by 2025, and there is the overall pattern utilizing the IoT. In IoT, information is gathered from different sensors, transmitted over remote systems, and afterward investigated. The detected and investigated information will

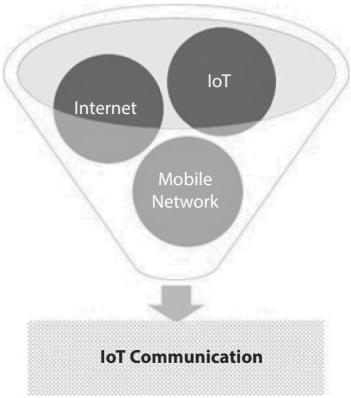


Figure 3.1 Process of IoT communication.

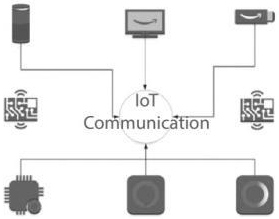


Figure 3.2 IoT communication devices.

be used to control actuators. IoT permits articles to be detected and controlled remotely or basically across existing system foundation, making open doors for more straightforward coordination between the physical world and PC-based frameworks, and bringing about improved proficiency, precision, and financial advantage [6]. IoT sense can allude to a wide assortment of gadgets, for example, heart checking inserts, biochip transponders on livestock, electric shellfishes in seaside waters, vehicles with worked in sensors, and DNA examination gadgets for natural/food/pathogen observing or field activity gadgets that help firemen in search and salvage tasks. These gadgets gather valuable information with the assistance of different existing innovations and afterward independently stream the information between different gadgets.

3.2 Features of IoT

Main features of the IoT include sensors, connectivity among various nodes, artificial intelligence, and smart devices. Some of the key features exist and are mentioned below:

1. Sensors: IoT uses various kinds of sensors which can get the information or data from numbers of nodes, connected with specific networks. This would get the data gathering between sensors devices and predict and addresses various system equipment [7]. Sensors are also reduced the human workload by collecting the information.
2. Connectivity: It enables the new networking devices connectivity process with a combination of IoT. So, networks would be acquiring the information whether it is based on a small or large network. IoT communicates with networks and sends the data. But connectivity is an important factor to utilize any IoT device.
3. Artificial Intelligence: IoT makes any process to be virtually and smart which would enhance the performance. Data collection using an artificial intelligence algorithm is efficient [8]. This technique is a smart process can utilize according to user need and trend concept.
4. Smart Devices: IoT uses various types of sensors to resolve the purpose of user requirements. These devices depend upon their need and cost constraints [9]. According to the IoT, the process uses smaller and cheaper and more powerful devices which would be beneficial for scalability and reliability.

3.3 IoT Sensor Devices

- Temperature Sensor
  A temperature sensor facilitates and measures the temperature and changes over it into an electrical sign. They have a significant job in the environment, agriculture, and industries. For instance, these sensors can recognize the temperature of the dirt, which is progressively useful in the creation of harvests. There are numerous kinds of temperature sensors and proficient, simple to introduce, and solid that reacts to human action [10]. The sensors take a shot