Chapter 15

Paradigms, Challenges, and the Future

Learning Outcomes

After reading this chapter, the reader will be able to:

- Assess the various evolving aspects and paradigms of IoT
- Understand the most prominent challenges encountered during the design and development of IoT solutions
- Research upcoming and emerging domains, which find significant applicability in IoT

15.1 Introduction

Since the inception of IoT, the technology has passed through multiple stages of development and revolutionized the industrial as well as consumer sectors rapidly. However, developers face multiple challenges while developing their ideas into reality. The IoT devices are usually resource-constrained in terms of their computational capability, battery power, as well as, storage. These limitations mandate the developers to develop routines that execute complex operations on the devices with ease, making IoT applications dependent on external platforms such as cloud and fog computing. Another significant issue is the rising number of IoT devices. IoT has penetrated diverse domains and extends its scope to smart homes, vehicles, cities, utility meters, and others. Such an increase in the number of interacting devices increases the consumption of resources and causes congestion in the network. In addition to that, the devices, along with their interconnections, have a non-trivial topology, which leads to complex networks. The IoT industries, therefore, need to develop new algorithms to deal with the increasing lattices in the complex network as well as multiple access protocols to avoid delays and packet drops. The increasing number of devices also consumes a lot of power, which calls for the development of new low-power hardware and schemes that involve smart energy harvesting and its consumption.

IoT devices include both static as well as mobile nodes, depending on the user's applications. Although mobility in such environments may or may not be random, developers need to be prepared for any pattern while providing their services. Since the precise prediction of mobility is challenging, it can only be analyzed statistically. Additionally, IoT environments also have multiple access points in close proximity. Such a deployment of access points creates interference, causing a reduction in signal-to-noise-plus-interference ratio (SINR) values, which causes a decline in signal quality and packet drops. IoT service providers need to impose smart channel selection as well as schemes to overcome these interferences. Developers also need to create new models to mimic the mobility of the users and propose schemes to facilitate smooth handoffs among the access points for uninterrupted service.

15.2 Evolution of New IoT Paradigms

As mentioned earlier, since the inception of IoT, it has successfully been used by multiple industries for running their operations and also providing their services to the users. IoT has found scope in diverse operations, which has led to the origin of several paradigms based on the nature of data sources/devices/peripherals and their corresponding applications. Some of these areas and the respective IoTs are explained in this section.

15.2.1 Internet of battlefield things (IoBT)

This category is responsible for connecting soldiers with IoT. Researchers in IoBT aim to develop a suite with embedded biometric and location sensors for soldiers. Data from these sensors allows the soldiers to keep track of the troops and also share information regarding foes; it makes the whole team situationally aware. Moreover, smart analysis using machine learning algorithms opens the scope for designing superior tactics in real-time. However, IoBT also has its challenges, mostly regarding energy constraints and data rates. Soldiers need to transfer sizeable data with minimum delay, which mandates the need for optimized consumption of bandwidth and battery. Finally, IoBT systems must be robust and durable enough to withstand the rigors of sustained outdoor and battlefield use.

15.2.2 Internet of vehicles (IoV)

This category of IoT is responsible for communications among smart connected vehicles, usually through vehicular ad-hoc networks (VANETs). Smart vehicles consist of a myriad of sensors that include cameras, GPS, infrared, and others. IoV facilitates these vehicles to communicate with other vehicles, its drivers, roadside units (RSU), and other mobile and fixed infrastructures. Intuitively, IoV supports intra-vehicle, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-cloud (V2C), and vehicle-to-pedestrian (V2P) communication. Although IoV faces a combination of challenges related to mobility, changing states, and dynamic signal quality, it has several advantages. Developers design IoVs such that they are environmentally safe, improve road safety, enhance user convenience, as well as, increase revenue of manufacturers.

15.2.3 Internet of underwater things (IoUT)

This category of IoT aims to interconnect underwater sensors and communication infrastructure with the terrestrial Internet. The sensor nodes in IoUT consist of smart devices and are usually powered by batteries. They are also much smaller in size than normal sensors and support wireless communication based on acoustic signals. However, IoUT has a significant lacuna in its communication model as radio waves do not fare well, underwater. Although developers use sizeable antennas for the signals to penetrate through water, the signals suffer high attenuation and absorption. Underwater, the signals also suffer from high propagation delays and bit error rates. Optical signals also seem impractical underwater due to the high absorption rate. Additionally, they can only cover short distances. Researchers, however, aggregate data from the sensors situated underwater to a sink node at the surface of the water, which forwards it to the terrestrial base stations in a multi-hop manner. The sink nodes in IoUT contains both acoustic as well as radio antennas for its purpose.

15.2.4 Internet of drones (IoD)

IoT operates toward enhancing user experience while minimizing user intervention. IoD is the category concerned with the deployment and management of unmanned ariel vehicles. Service providers use IoD for various applications such as package delivery, wildlife surveillance, rescue operations, agriculture, photography, and others. However, developers need to deal with flying the drones in controlled/uncontrolled airspace and dictate navigation coordinates. For the seamless operation of IoD, developers need to fuse air traffic control networks, cellular networks, automation, and the Internet [1].

15.2.5 Internet of space (IoSpace)

This category of IoT relies on low earth orbit (LEO) satellites for providing seamless connectivity services over uneven demographic areas. However, such satellites have disadvantages concerning development and deployment cost, and loss due to failure in orbit. These satellites have the potential to reduce network latencies significantly.

Researchers have been recently working hard toward the development of small cubic satellites called CubeSats to overcome the challenges mentioned here [2]. In addition to these difficulties, satellites also present challenges related to tracking, synchronization, and handoff. We expect that technologies such as software defined networks (SDN) and network function virtualization (NFV) will play a major role in addressing these issues.

15.2.6 Internet of services (IoS)

This category is specific for manufacturers and service providers, that is, the industries. With IoS, manufacturers bring hardware and software under one umbrella. For instance, a car manufacturer builds a car with installed sensors. They later release software updates over the Internet to enhance user experience. The manufacturers may also charge for the upgrades, which generates revenue for the company. Additionally, this model also paves the way for crypto-currency as a payment method. Applications of IoS extends to factory monitoring, sensing and actuation of factory units, and generation of remote alarms in case of emergency. IoS also reaches out to smartphones that already have multiple sensors. Companies use these sensors and develop Internet-enabled apps for users.

15.2.7 Internet of people (IoP)

The Internet contains a plethora of profiles representing people and interconnected links as relations among them. The IoP interconnects these peer-to-peer networks. Researchers in social computing extensively use social graphs for representation and inferences. The IoP supporting applications facilitate direct device-to-device, people-to-people, as well as company-to-people communications. IoP further opens scope for crypto-currency as a means to transfer incentives/payments in return for services. Such structures enable smooth interaction among service providers and consumers. IoP also provides a platform for carrying out transparent and secure payments.

15.2.8 Internet of nano things (IoNT)

The interrelated systems in IoT, which usually include combinations of sensors and actuators, can be miniaturized to tiny devices with dimensions in the scale of nanometers. These devices are application-specific and occupy minimal space; they include miniaturized sensors in vehicles, as well as those responsible for monitoring the environment. Communication at the nano-scale is rendered possible in two ways: 1) electromagnetic (EM) and 2) chemotaxis communications. Electromagnetic communications at the nano-scale typically use the Terahertz band of the spectrum. However, this results in significant power issues, a limited range of communication, and severe susceptibility to interferences. Parallelly, the use of chemotaxis as a means of communication is achieved through exploiting the population dynamics of bacteria and viruses. Messages are passed in the form of chemical signatures and molecules, which are often facilitated by specifically cultured bacteria and viruses. Nano-scale IoT also finds scope in healthcare, where researchers are working actively in fighting diseases with the help of programmable bacteria/viruses/nanoparticles. However, designing such nanodevices is a non-trivial task, which the developers need to study rigorously.

15.2.9 Internet of everything (IoE)

The IoE comprises four pillars and concerns itself with the communication among them. These four pillars are people, data, processes, and things.

(i) People: Communication among people is analogous to the IoP mentioned earlier.

(ii) Data: Data from sensors are analyzed for inferencing and making decisions.

(iii) Process: Information is delivered to the concerned people/machine/infrastructure.

(iv) Things: This is analogous to the things in IoT.

The main difference between IoT and IoE is that IoT only concerns itself with the non-human aspects of technology, while IoE consists of all the other factors, which include machine-to-people (M2P) and technology-assisted peer-to-peer (P2P) interactions in addition to the features of IoT.

15.3 Challenges Associated with IoT

IoT has numerous advantages up its sleeve. However, with the advent of these technologies and heterogeneity of the nature of devices, IoT also has several challenges that researchers are trying to overcome actively. In this section, we mention a few such challenges.

15.3.1 Mobility

IoT supports unconditional M2M communication. The devices in the system, given their heterogeneity concerning configurations and usage, that is, pedestrians, vehicles, cycles, drones, robots, and others, have diverse mobility patterns. These patterns cannot be precisely predicted and need to be stochastically analyzed, which makes efforts toward seamless connectivity and quality of service tricky. Developers need to devise ways to make dynamic decisions on the handoff, synchronization, and others such issues efficiently. Tasks such as allocation of identifiers to mobile devices, handoff strategies, coverage estimation, path planning, mobility prediction, and others are some of the research domains which are directly associated with addressing this challenge.

15.3.2 Addressing

With the advent of IoT and its advantages, its adoption by the people as well as, industries are growing at an uncontrollable rate. Such an exponential increase in the number of devices exhausts the number of available IP addresses, leading to IP conflicts. In addition to that, there are very few standards or industry-recommended schemes toward addressing IoT administrators. Recently, IoT has already seen a paradigm shift from IPv4 to IPv6 addressing schemes in some industries but it is yet to be popularly adopted by the masses. Typical research challenges in this domain include addressing strategies, sub-netting strategies, and others.

15.3.3 Power

IoT devices are usually resource-constrained concerning power and computational capability. These devices need to last for a long time irrespective of their limited battery power. Such limitations call for green computing schemes for smart harvesting and consumption of power. Alternatively, it also calls for new hardware designs that consume minimum power for operation. Various upcoming research solutions focus on developing high-density batteries/cells for enabling long-term use of IoT systems. Research in this domain includes the design of low-power processors and hardware, design of low-power consuming computation techniques and algorithms, energy harvesting, alternative sources of energy, and others.

15.3.4 Heterogeneous connectivity

IoT is a vast collection of heterogeneous networks made up of long-range, as well as, short-range connectivity technologies. Some of the integrated sectors in IoT also rely on their own proprietary connectivity solutions. The proprietary nature of connectivity is commonly encountered in applications such as military, heavy industries, and others. Heterogeneity in connectivity can be significantly challenging to manage as often connectivity devices may be vendor-specific, industry-specific, or even task-specific. Some antennas may be more powerful than the others, or maybe close to one another, inducing high interferences. Coverage is also an issue in such environments. Additionally, as the devices move away from access points, they may lose contact midway, which is an open problem so far. For example, the majority of connectivity technologies are still present in industries are wired. Despite the high maintenance costs and physical space occupancy, wired solutions are considered more reliable and secure for industrial uses. Additionally, legacy connectivity technologies are still present in industries and they are majorly wired and mostly analogous. These industries and industrial systems need to be connected to the Internet. The main challenge in such situations is the amalgamation or provision of a unified solution which can handle analog as well as digital content, and that too for different vendor-specific devices and protocols. Typical research in this domain consists of work on protocol conversions, bandwidth allocation, task offloading, big-data analytics, cloud computing, and others.

15.3.5 Communication range

The wide expanse and reach of IoT have led to some of its major challenges, addressing which have given IoT some powerful new solutions. The usefulness of IoT has led to its solutions being deployed in areas with proper connectivity as well as areas, especially remote ones, where there is barely any connectivity. Both of these scenarios have their own unique set of challenges, which need to be addressed separately. For example, the deployment of low-power wireless IoT solutions in urban areas tend to frequently encounter interference and noise due to the presence of other powerful wireless solutions operating at the same frequency spectrum. In contrast, the deployment of IoT solutions in remote places such as forests and rural areas often do not have the proper network infrastructure to provide these solutions with basic Internet access. The rise of IoD in providing communication coverage to such areas through relaying of signals, enabling backhaul network access, and others is a prime example of a powerful, yet economical solution rising due to the communication demand–supply gap in IoT.

15.3.6 Security

Due to the lack of powerful and unified security standards in IoT and an increasing number of devices, IoT is vulnerable to threats from malicious attackers and bots. Although encryption seems to be a logical answer in this scenario, a significant chunk of these devices lack the storage and computational capabilities required for supporting complex mathematical operations, which come with encryption. Some manufacturers put a built-in password for security, which is temporarily helpful in a few limited scenarios. However, attackers have enough resources to crack such default passwords, which compromises the whole system. IoT is not restricted to low-power devices, and even so, these low-power devices eventually connect to remote platforms such as a server/fog/cloud. Gaining access to the network or the remote infrastructure by compromising the low-power devices is a reality in the present-day technological realm. Vulnerability to attacks such as phishing, flooding, denial of service, man-in-the-middle attacks, and others, can easily trigger a chain of anomalies, which may bring down a whole network or enterprise. Typical research in this domain includes works on hardware-level security, processor/chip-level security, physically unclonable functions (PUFs), network security, cryptography, blockchains, crypto-currency, encryption, and others.

15.3.7 Device size

Manufacturers usually design IoT devices for enhancing user experience at low cost. Further, such devices are usually small in size, equipped with unique IDs and wireless communication antennae. The low cost and size make it difficult to incorporate processing power and storage in the device. It also causes space concerns to introduce a battery. Finally, these devices end up being resource-constrained in terms of operational capability, battery power, and storage. Typical research in this aspect of IoT includes nano and microelectronics, photonics, device fabrication, and the new and upcoming paradigm of quantum computing.

15.3.8 Interoperability

IoT devices serve a myriad of applications with numerous manufacturers deploying multiple units. These devices with different purposes and different manufacturers need to interact with one another to work in harmony. With the increasing number of devices and no universal standards, researchers are working actively to enable the devices to achieve common goals automatically. Chapter 9 on interoperability covers the various aspects associated with this challenge.

15.4 Emerging Pillars of IoT

IoT is a massive paradigm with far-reaching implications across vastly interdisciplinary domains. However, some standalone paradigms, are nowadays commonly associated with IoT due to the benefits of association these technologies bring to themselves as well as to IoT. We discuss some of these emerging pillars of IoT in the subsequent subsections.

15.4.1 Big data

Manufacturers and users are deploying numerous IoT devices while serving a plethora of applications. Along with these IoT devices and applications, the rate of data generation also increases, leading to large datasets (petabytes or gigabytes). These data may be structured/unstructured; developers need to analyze these data for finding hidden patterns and generating inferences. For comprehending these inferences and decisions, developers are turning toward big data analytics. The network traffic or data is classified as big data if it satisfies specific characteristics of 1) volume, 2) variety, 3) value, 4) velocity, and 5) veracity. Big data analytics has the potential to process data from IoT devices in real time and store them using various storage schemes. Once acquired, this voluminous data can be used for studying patterns in network behavior, usage, customer experiences, mobility, connectivity issues, among many other interesting features [3].

15.4.2 Cloud/fog/edge computing

Commerical device manufacturers design IoT devices and solutions for providing affordable services to the general public. Specific use cases of IoT, such as those for industries, militaries, and other such applications, are also catered to, mostly through proprietary solutions. However, the sheer volume and variety of data that is available for further processing needs powerful resources and infrastructures. Although a significant number of IoT devices are smaller in size and resource-constrained, their massive-scale use in various applications eventually leads to a formidable amount of information to be processed and handled. Due to such limitations, these IoT devices need to depend on external platforms, particularly cloud/fog/edge computing [4] [5] schemes, to address their processing issues and generate meaningful information from the gathered data. The choice of platform is application dependent, that is, while cloud computing has unlimited resources, fog/edge computing reduces operational latencies significantly. Starting as a research paradigm, these domains have gathered worldwide acceptance and are mostly included in mainstream IoT architectures and applications.

15.4.3 5G and beyond

The launch of 3G technology facilitated robust and speedy voice, text, and data services to the users. 4G was similar to 3G but with a higher data rate, enabling its users to adopt video-based communication and making it a new normal in the communication industry. The new 5G technologies provide services with much higher speeds, as they focus on providing ubiquitous high-speed connectivity to all device types. Features such as downloading full HD movies in a matter of seconds characterize this technology. 5G technology features a fusion of high data rates with low latencies, ubiquitous coverage, and smart infrastructures to support real-time applications, enabling remote monitoring and control [6]. Researchers envision 5G as a driving force for IoT. The features of 5G have also started the race for beyond 5G technologies and paradigms. Envisioned as operating in the Terahertz band of the frequency spectrum, beyond 5G technologies are being speculated to have data rates in the tune of Gbps [7].

15.4.4 Artificial intelligence (AI)/Machine learning (ML)

Owing to the deployment of numerous IoT devices and applications, the complexity and size of data over and beyond the networks have increased significantly. The IoT data may or may not be structured and often consists of hidden patterns, which have to be derived through data processing and statistical inferences. Modern-day AI/ML-based tools have significantly powerful inferencing procedures, which can outperform almost any of the standard statistical methods. Additionally, the need for automation in a significant chunk of IoT devices and applications is another compelling reason for the rapid emergence and adoption of AI/ML with IoT [8]. AI/ML has been used for extracting information from raw data, be it from agricultural sensors, smart home sensors, or network security analyzers. AI/ML tools are mostly data-driven. However, new methods in these domains are rapidly cropping up; methods which do not always have to rely on voluminous data for generating inferences or predicting trends.

15.4.5 Cognitive communication networks

This domain is yet another upcoming pillar of IoT, which, although focused only on the communication aspects, has the potential to revolutionize the existing IoT architectures and the way data and signals are handled in a network. Cognitive communication networks or simply, cognitive networks are capable of sensing the present network's parameters, conditions, and plans. Based on the sensed information, the cognition engine can devise pathways and strategies for best achieving the end goals for a certain task. For example, an IoT node transmits data to a remote server through a fixed gateway, which has access to the Internet. However, this gateway also serves 10,000 other such IoT nodes. The situation undoubtedly raises the issue of congestion at the gateway (considering normal channel bandwidth) due to large waiting message queues. As the traditional IoT networks are designed to follow somewhat similar architectures, the load on networks is highly unbalanced and unevenly distributed. This uneven traffic load also results in long waiting times, packet drops, and noise in the data being transmitted over the network. Now consider a smart network which can sense delays and queues in a certain path and has the autonomy to choose an alternative path to facilitate data transmission between the IoT node and the remote server. This mechanism can be considered as a rudimentary example of a cognitive network.

15.4.6 Network function virtualization (NFV)

NFV is an interesting and practical concept, which proposes the virtualization of major network elements such that software virtualizes network hardware by providing the same functionalities and added features. The concept of NFV arose due to the difficulty of reconfiguring (both changing and upgrading) installed network infrastructures. Physically going to every network element for changes (updates, software patches) can be a significant challenge in terms of time, money, and human resources, especially for enterprise-grade networks consisting of tens of thousands of network elements. NFV utilizes the concept of virtualization to provide services similar to network elements through standard servers.

15.4.7 Software-defined networks (SDN)

IoT environments are highly dynamic concerning mobility and the changing states of the access points. With the implementation of fog and edge computing, the states of the service providing nodes will change; so will the users. For the seamless transition of data routes, self-organization, configuration optimization, and smart transmissions, SDN has emerged as a popular choice. SDN reduces the complexity of traditional networks by introducing a centralized control structure through the separation of control and data planes of network elements. A centralized view of the whole network ushers in the benefits of better controllability, network stability, and increased efficiencies. It is to be noted that SDN and NFV are separate paradigms. NFV simply virtualizes the network elements in a traditional network, such that the core operating procedure remains the same. In contrast, SDN introduces an entirely new way of handling network traffic by separating the control and data planes to provide a centralized architecture for the whole network.

15.4.8 Phantom networks

"Phantom networks" paradigm strives to develop intangible communication infrastructures. Being a relatively new paradigm, which is still under development, this paradigm relies on the Terahertz (THz) band for communication between aerially diffused nano-relays. The aerial nano-relays are deployed through ground-based pumps, which spray the water-suspended mixture of the nano-communication relays in the deployment area. However, unlike traditional network infrastructures, this paradigm is prone to the effects of wind, rain, humidity. Additionally, the factors of node density in an area to ensure reliable throughput and quality of service and settling time of these aerially suspended nodes play decisive roles in deciding the network lifetime and performance of the network. This paradigm is highly interdisciplinary and requires the operational knowledge of multiple domains such as nanotechnology, communication, networking, fluid dynamics, and others. Typical application areas include military communication and communication for emergency response during disaster management.

Summary

In this chapter we discuss the present challenges and upcoming paradigms associated with IoT.

Exercises

(i) What are the new evolving paradigms as a result of the use of IoT in various domains?

(ii) Discuss the salient features and differences between the Internet of vehicles and the Internet of drones.

(iii) What are the common challenges associated with the adoption of IoT in any new domain?

(iv) How is NFV different from SDN?

(v) What are the challenges associated with beyond-5G communication?

(vi) Discuss the role of AI/ML in IoT.

(vii) How is cognitive communication poised to enhance the usability of IoT networks?

(viii) What are the typical features of a data for it to be characterized as big data?

(ix) How is cloud-based storage different from regular offsite storage in IoT networks?

References

[1] Gharibi, M., R. Boutaba, and S. L. Waslander. 2016. "Internet of Drones." *IEEE Access* 4: 1148–1162.

[2] Akyildiz, I. F. and A. Kak. 2019. "The Internet of Space Things/CubeSats." *IEEE Network* 33(5): 212–218.

[3] Fahad, A., N. Alshatri, Z. Tari, A. Alamri, I. Khalil, A. Y. Zomaya, S. Foufou, and A. Bouras. 2014. "A Survey of Clustering Algorithms for Big Data: Taxonomy and Empirical Analysis." *IEEE Transactions on Emerging Topics in Computing* 2(3): 267–279

[4] Bera, S., S. Misra, and J. J. Rodrigues. 2014. "Cloud Computing Applications for Smart Grid: A Survey." *IEEE Transactions on Parallel and Distributed Systems* 26(5): 1477–1494.

[5] Sarkar, S., S. Chatterjee, and S. Misra. 2015. "Assessment of the Suitability of Fog Computing in the Context of Internet of Things." *IEEE Transactions on Cloud Computing* 6(1): 46–59.

[6] Agiwal, M., A. Roy, and N. Saxena. 2016. "Next Generation 5G Wireless Networks: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials* 18(3): 1617–1655.

[7] Huq, K. M. S., S. A. Busari, J. Rodriguez, V. Frascolla, W. Bazzi, and D. C. Sicker. 2019. "Terahertz-enabled Wireless System for Beyond-5G Ultra-fast Networks: A Brief Survey." *IEEE Network* 33(4): 89–95.

[8] Poniszewska-Maranda, A., D. Kaczmarek, N. Kryvinska, and F. Xhafa. 2019. "Studying Usability of AI in the IoT Systems/Paradigm through Embedding NN Techniques into Mobile Smart Service System." *Computing*: 101(11): 1661–1685.