SPRINGER BRIEFS IN
ELECTRICAL AND COMPUTER ENGINEERING

Fatima Hussain

Internet of Things
Building Blocks and Business Models

Springer

SpringerBriefs in Electrical and Computer Engineering

More information about this series at http://www.springer.com/series/10059

Fatima Hussain

Internet of Things

Building Blocks and Business Models

Springer

Fatima Hussain
Assistant Professor
School of Computer Science
University of Guelph
Guelph, ON, Canada

Research Associate
Department of Computer Science
Department of Electrical and Computer
Engineering
Ryerson University
Toronto, ON, Canada

ISSN 2191-8112 ISSN 2191-8120 (electronic)
SpringerBriefs in Electrical and Computer Engineering
ISBN 978-3-319-55404-4 ISBN 978-3-319-55405-1 (eBook)
DOI 10.1007/978-3-319-55405-1

Library of Congress Control Number: 2017935480

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

I dedicate this book to all of my teachers and mentors from Kindergarten to PhD.

Foreword

With the increasing demand for connectivity of everything, the Internet of Things (IoT) has now become a key technology that spans multiple technology domains from data sensing to networking to data analytics. We are now becoming accustomed to our daily activities either at homes or offices being interconnected via smart devices to the outside world. In this book, the integration of core building blocks of IoT such as sensing, processing, communication and networking is covered in a simple approach with real-world applications. This book is a good reference source for beginners to understand how the traditional network-centric domain emerges as a device-centric domain in IoT platform. It covers basic IoT building models with emerging applications and services, supplemented with advanced concepts such as fog computing and cooperative IoT network. Nicely blending technology with business to give a practical and entrepreneur sense of the IoT paradigm, this book also covers emerging trends and research challenges in distributed and autonomous IoT functionalities. Readers will understand the practical challenges of integrations, deployment and security and learn some basic design principles in IoT. This book is a good reference resource for graduate students, researchers and industry practitioners working in the IoT field.

Dr. Alagan Anpalagan
Director, WINCORE Lab
Professor, Department of Electrical
and Computer Engineering
Ryerson University, Toronto, ON, Canada
E-mail: alagan@ee.ryerson.ca

Foreword

Arguably, the first Internet of Things (IoT) application debuted on the 22nd of November 1993 when a camera at the University of Cambridge was aimed at a coffee pot to provide several computer science researchers, located on a different floor, some indication of when the coffee would be "on". We have come a long way-often in fits and starts. Today, the various technical communities have agreed on protocols, algorithms and techniques that have been translated into standards that do not simply allow the Internet to exist but provide impetus for new applications involving more and more "things" to take advantage of its ubiquitous nature. Dr. Hussain's work provides an important introduction to the key components of what IoT is today with insight into what it may become in a promising future.

Dr. Alexander Ferworn
Vice Chair of Senate
Liaison, Faculty of Science and Faculty
of Engineering and Architectural Science
Director, NCart Lab
Professor, Department of Computer Science
Ryerson University, Toronto, ON, Canada
E-mail: aferworn@scs.ryerson.ca

Acknowledgements

I want to thank Dr. Anpalagan for reviewing this draft and giving valuable suggestions. I also want to thank Dr. Ferworn for his endless moral support and encouragement.

Contents

Chapter 1
Internet of Everything

Fatima Hussain

1.1 Introduction

Internet of Things (IoT) can be defined as "interconnection of things" used to sense and report real world information. The applications and usage of the internet is expanding on a daily basis and IoT is the new approach for incorporating the internet into personal, professional and social life. IoT can be seen as connected set of anyone, anything, anytime, anyplace, any service, and any network. It is envisioned as billion of sensors connected to the internet that will generate large amount of data which need to be analyzed, interpreted and utilized. The term 'Internet of Things' or 'Internet of Objects' represents various kinds of devices having varying sizes and capabilities, that are connected to the internet [1]. By expanding these current internet services, we will be able to accommodate every object present across the globe. Originally, IoT was used to refer to uniquely identifiable, interpretable connected objects enabled with radio-frequency identification (RFID) technology. Afterwards, sensors, actuators, GPS devices, and mobile devices were linked to it. Commonly, IoT is defined as;

> A dynamically changeable and self configurable, global network infrastructure having special characteristics based on interpretable communication protocols. In this infrastructure, physical and virtual "things" are intelligent

(continued)

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_1

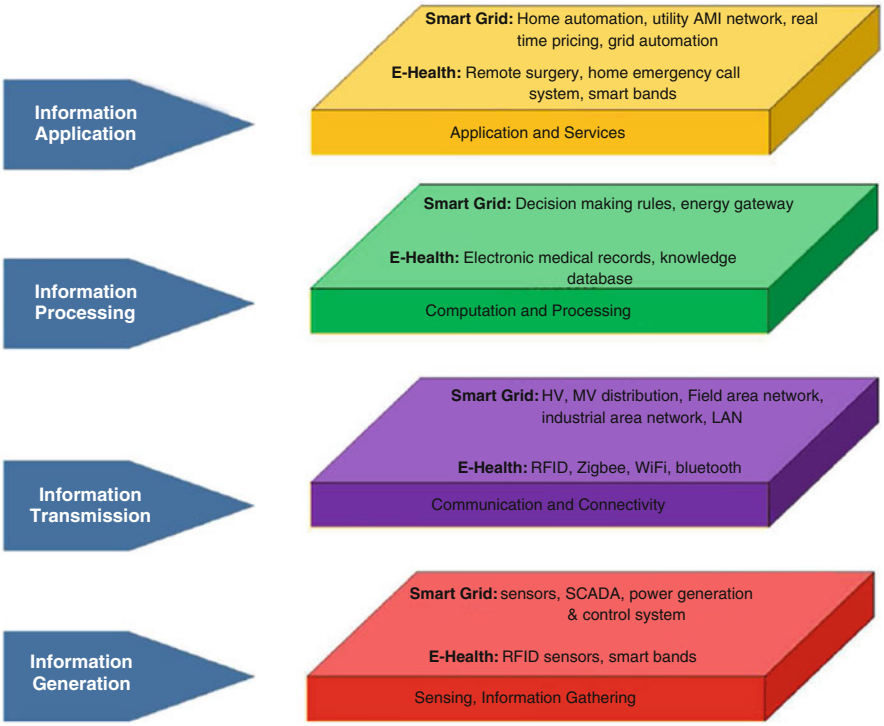

Fig. 1.1 Building blocks

and have unique identities, physical attributes, and are seamlessly integrated into the information network [2].

Potential benefits of IoT are almost limitless and new IoT applications are evolving every day. Imagine millions of sensors connected to one another and tons of data being extracted from these sensors. IoT potentially extracts and analyses this data and applies to automated process for various applications. We can also define it as an integrated technologies providing new exciting solutions and services to people.

Concept of IoT can be better explained by four blocks as shown in Fig. 1.1. Understanding these IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. All the chapters in this book are designed based on these blocks. These include sensing, communication, computation and service [3].

IoT Sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices.

For instance, these include RFIDs sensors for e-health applications, and SCADA, power sensors for smart grid networks.

IoT Communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, IoT devices are required to operate at low power. Examples of communication protocols used for the IoT are WiFi, Bluetooth, Zigbee and LTE-Advanced. Some specific communication technologies are considered useful for IoT, like RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB) for proximity services.

For example, for smart grid application, high voltage/ medium voltage distribution network and industrial area network are examples of communication networks, to interconnect smart grid power system equipments. While for e-health Zigbee, RFIDs and WiFi are used for signal exchange among various health monitoring sensors and devices.

IoT computations can be divided into two major categories. One deals with the processing and execution of various commands. Another deals with the data storage and processing.

- **Processing Units** is the operating system or a "brain" of IoT and represents its computational abilities. It includes micro-controllers and microprocessors. There are several real time operating systems which are good candidates for the development of real time IoT applications.
- **Cloud Units** act as a storage space for big data collected from processing units of IoT. It facilitates smart objects and devices to send their data to cloud. There is where real time processing is done and useful knowledge is extracted form this collected data. There are lots of free and commercial cloud platforms and frameworks available nowadays to host IoT services.

For instance, these functions of computation and storage is done by decision maker and energy gateways in smart grid applications and electronic medical record data base in e-health scenario (Fig. 1.1).

We can categorize IoT services into four classes:

- **Identity Related Services** are the most basic and important services that are used in other types of services. Every application that needs to bring real world objects to the virtual world has to identify those objects.
- **Information Aggregation Services** collect and summarize raw sensory measurements that need to be processed and reported to the IoT application.
- **Collaborative Aware Services** act on top of information aggregation services and use the obtained data to make decision and react accordingly.
- **Ubiquitous Services** aim to provide collaborative services anytime by anyone, anywhere.

For example, services provided buy smart grid networks are home automation, utility AMI network, real time pricing etc. In case of e-health, remote surgery, real time health monitoring etc. are few services to name.

In the rest of this chapter, we will introduce and present various building blocks of IoT. In rest of the book, various chapters will provide insight on state of the art research and innovation in various building blocks of IoT.

1.1.1 IoT Traffic

IoT traffic patterns are different from traditional traffic and also versatile in nature. We briefly discuss how IoT traffic is different from traditional one. As knowledge of traffic patterns and nature plays an important role in design of network architecture and protocols. It is also important to know the quality of service requirements of specific IoT applications, as traffic characterization strongly depends upon application area. By knowing statistical nature of IoT traffic, we are able to design IoT networks for transparency (predictability) and accessibility of QoS requirements.

1.1.1.1 Communication in Close Proximity

IoT networks have broadened the concept of conventional network-centric system to device-centric mobile system, where the devices in close proximity are allowed to communicate with each other while bypassing the base station. The design of the earlier mobile communication systems was based on the implicit assumption that users are not in close proximity with one another and follow the traditional notion

of a cell, base station, uplink, and downlink. However, with the proliferation of many new applications such as online gaming and social networking, it has been observed that interaction among the users in close proximity happens more frequently and IoT encompass and embrace this evolved vision.

1.1.1.2 Ultra-Reliable and Low Latency Communication

Traditional networks can be thought of as human-centric, i.e., the design of these networks is meant for human to human (H2H) communication. Therefore, in these networks, the reliability and latency are considered from the perspective of human users. However, IoT networks will provide native support for machine to machine (M2M) communications besides supporting H2H communication. Hence, a number of mission critical application scenarios, e.g., industrial process automation, remote surgery, and intelligent traffic transport system needs to be considered. However, these new IoT applications will require very high reliability, availability everywhere and all the time, and low end to end latency as compared to the today's communication system.

1.1.1.3 Low Power/Low Cost Communication

H2H communication is the main objective behind traditional communication systems. Thus, it includes the devices which do not need any extremely stringent constraint in terms of power consumption, because they can be recharged on a daily or weekly basis. However, IoT systems will support a number of smart applications, e.g., smart metering and smart load balancing for appliances, which consists of a massive number of low-cost sensors and actuators. These devices are characterized by low data rate, low power consumption, and low cost, so that a huge number of devices can be deployed to improve the efficiency of monitoring and actuation performed by these devices such as in case of power systems. Such applications should be extremely energy efficient which is beyond the provision of the today's communication systems.

1.1.1.4 Urgent Communication

Few IoT applications require temporary and urgent network of devices. Such temporary network can be highly beneficial to fulfill the need of urgent communication in case of emergency or disaster situation e.g., earthquake or hurricane etc. These networks need to be setup and maintained in a very short interval of time, therefore, impose stringent requirements in terms of self-organization and self-healing, which has never been considered in existing mobile communication networks.

1.2 Building Blocks

1.2.1 Sensors and Machines

Integration of sensors/actuators, RFID tags, and communication, and technologies leads to the formation of IoT networks. It is comprised of interconnected smart objects/devices, cooperating and communicating with one another to achieve mutual tasks [2].

These "smart" objects have sensing, actuating, and data processing capabilities, and may be comprised of one or more embedded sensors. These smart objects have a potential to sense/capture enormous amounts of data, and this sensing as a service model is built on top of the IoT infrastructure. Users can buy these smart sensers or can rent through middle-ware solutions such as OpenIoT and GSN. Middle-ware solutions are meant to interconnect sensors to back-end software systems.

There are couple of challenging tasks present in the successful sensor deployment. Most important challenge is the choice of IoT solution and in turns sensor selection. Traditional web based search techniques will not work in this regard, as it cannot fully reflect critical characteristics of sensors.

Wireless sensors are the most appropriate choice for IoT networks, but all of these sensors are battery powered. Therefore, they are constrained in energy and battery life. Energy and power maintenance is another challenge for sensors' operations such as, data sampling/ processing and radio communications. In addition to this, supplying reliable power to the sensors, for a prolonged period of time, is a key to loT being deployed successfully. This is especially a major concern, when these sensors are employed in remote and distant locations such as below under earth surface or in space. As it is not feasible to change batteries for these devices, energy must be harvested from the environment. In addition to this, energy must be conserved by minimizing the cost for sampling and processing, to prolong the network lifetime.

Useful data extraction and interpretation from huge amount of sensed and received data is very challenging. For different applications, it might be the case, that sensor reading from specific area are temporally correlated. Differen data fusion techniques can be used, to improve the collected data quality, by exploiting the spatial correlation [4].

Heterogeneity of data from versatile IoT devices raises inter-operability issues among their format and measurement procedures. Managing this enormous amount of data and related inter-operability is another challenge for IoT sensor networks. There are various types of sensors which can be used in various IoT applications. It can be light, sound, acoustic or magnetic sensors and will be discussed in more detail in the next chapter.

1.2.2 Interconnecting Technologies

IoT is an pervasive network and capable of delivering innovative application and services to mankind. An effective execution of these services requires reliable telecommunication infrastructure. As IoT is a global network infrastructure, having blocks of sensor devices rely on networking and information processing technologies, for data exchange. Eligible communication technology may include from limited area network such as Zigbee, cellular networks to emerging long range facilities. RFID technology is considered as foundation for IoT, in which microchips are used to read the information and communicate wirelessly to near by server. Wireless sensor networks (WSNs) can also be considered as an important foundation for IoT, as it mainly interconnects smart sensors to sense and report. IoT devices employ a broad array of networking protocols and versatile applications and network domains.

The widespread popularity and deployment of IoT is supported by interconnection of smart objects and devices, with various types of wireless technologies [1]. It covers various protocols like LTE, 3G, WiFi, and WiMax etc. Different IoT networks have different demands in term of connectivity, therefore, there is no single solution that fits all. If high bandwidth with more data rate is required then WiFi is suitable, as it also provides the non line of sight transmission facility. For low data rate, close proximity IoT applications, Zigbee suits well. Similarly, real time applications have different data rate and delay requirements compared to scheduled or periodic reporting ones [5].

These technologies can be divided broadly into three categories [6]:

Non-IP Technologies do not use internet protocol for data exchange such as Zigbee, Insteon and Z-wave.

IP-Enabled Technologies require unique IP addresses for transmitting data over the network such as WiFi, VPN and LoWPAN etc. IETF group developed IPv6 over low power wireless personal area networks and is recommended for small area IoT networks.

High Level and Middle-Ware Protocols are used by energy constraint devices for communication purposes. Two of these are recommended in resource constraints scenario, and these are constrained application protocol (COAP) and global sensor network (GSN).

1.2.3 Big Data and Fog Computing

The smart devices in IoT networks create huge amount of data sets containing various types of valuable information. Peripheral devices such as sensors in IoT network produce large amounts of data, which is used to infer knowledge [7]. One of the major challenges is to handle this vast amount of data, however, solutions to these technical issues and challenges for handling this data, have emerged in recent

years. IoT also inherits several signal processing problems namely, data fusion, data abstraction, and data summarization. For analyzing this huge amount of big data, sophisticated sampling, quantizing and extraction technologies are needed.

1.2.3.1 Cloud Computing

Cloud computing is a platform that is expected to handle and manage this huge amount of data generated by IoT devices [8]. Cloud computing offers accessing the stored data from anywhere, anytime, and afterwards expanding the services independent of end user hardware. Cloud computing presents numerous benefits compared to conventual computing in terms of cost, scalability, performance and maintenance.

Therefore, cloud-centric IoT architecture will provide storage and computing resources for aggregated sensed data. Afterwards, techniques of data analytics and data mining are applied for information retrieval and knowledge discovery on collected data by IoT sensors.

1.2.3.2 Fog Computing

New evolving IoT applications require a platform with unique characteristics. Although cloud model seems useful for IoT applications but is not unanimously useful, due to it's limitations in terms of latency and distributive coverage. Fog computing assists and supports the cloud to handle this large amounts of data generated by IoT.

The term big data is coined with three dimensions: volume, velocity, and variety. When we bring in fog, we are adding fourth dimension to this data. This fourth dimension is the geo-distribution of various smart devices. Fog refers to distributed smart platform near user-end and which is capable of networking and storage of resources, distributively. It uses a localized computing model to communicate with end-devices rather than the data being routed over the whole internet backbone [3]. Fog is an intermediate layer that increases reliability and reduces latency. For instance, important parameter in the measurement of air quality and pollution level, will be the number of sensors distributed throughout the smart city [9]. In this scenario, data rate of individual sensor or amount of data generated will not be important. In short, fog computing provides minimized latency, bandwidth conservation, improved security, and reliability.

Cloud computing is brought to the user-end with the help of the fog. Same networking, computing, and storage resources are used by cloud and fog. Even they use same mechanisms and attributes like virtualization and multi-tenancy. It accelerates awareness and response to event by eliminating round trips to the cloud for analysis. There are few of applications that do not suit cloud environment and it leads to conception of fog concept. It includes but not limited to:

- Latency constraint application such as online gaming and video inferencing etc.
- Fast moving smart applications like vehicle-to-vehicle communication, smart rail etc.
- Large scale geo-distributed control systems such as smart transportation, intelligent traffic and signal light systems. It also includes environmental monitoring systems spanning large areas.

1.3 Applications and Business Models

1.3.1 IoT Applications and Use Cases

We can have countless IoT applications in our everyday life around the globe. Presently, it becomes lot easier to network smart objects with each other, due to advancement in sensors and wireless technology. Some of the most commonly deployed applications include;

- Home automation and security that may include smart grid, appliance control, light management etc.
- Industrial automation and management of manufacturing equipment and assets.
- E-Health system spanning from blood pressure, heart rate monitoring to remote surgeries.
- Environmental monitoring including air, water quality, soil, wildlife monitoring.
- Infrastructure management and monitoring of urban and rural assets.
- Smart transportation system including smart parking, smart traffic control, vehicle to vehicle communication etc.
- Industrial projects in food industry, agriculture, surveillance etc.

1.3.2 IoT Business Models

IoT is a mega trend in next generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of identifiable smart devices with extended benefits. With rapid progress and innovation in intelligent computing industry and information processing, IoT is evolving and flourishing as a new industrial reform.

Since IoT industrial reform does not only depend upon new innovations in IoT industry but innovative business models are also required. Unfortunately, development levels of IoT application innovation and business models are not in the same pace. Also, its challenging for designers to maintain a balance between potential benefits and deployment cost for IoT industrial application development.

A systematic connection is required between these two innovations i.e., for technology and business model for IoT industry to progress. We consider technology innovations to be the driving force behind the industrial IoT merchandise.

1.4 Book Organization

This book is comprised of five chapters (Fig. 1.2). This first chapter gives the introduction of IoT. In Chap. 2, we discuss and summarize various types of IoT sensors and mode of communication between them. We also discuss cooperative mode of operation in sensors and present respective performance analysis in IoT networks.

In Chap. 3, we discuss big data generated from IoT devices/applications and related challenges. We also discuss suitability of cloud and fog computing for specific IoT applications and elaborate their interplay.

In Chap. 4, we present the recent research in IoT from domestic and industrial perspective. We present some key applications of IoT and possible research area for future academic and industrial researchers. Afterwards, we analyze the role that the internet has played in business models to date, and also document the specific economic energy of IoT and patterns of IoT business models.

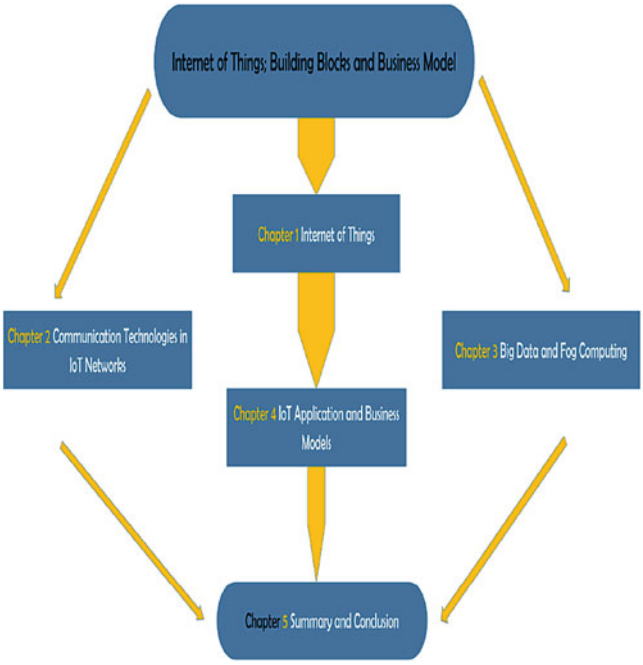

Fig. 1.2 Book organization

In Chap. 5, we summarize the main points and ideas presented through out the book. Recent research and open research challenges, in major IoT blocks is also given. At the end few research problems are identified along with suggested solutions.

References

1. Miraz, M. H., et al. (2015). A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet ofNano Things (IoNT). In *IEEE Internet Technologies and Applications* (pp. 219–224).
2. Xu, L. D., & He, W. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*, 2233–2243.
3. Al-Fuqaha, A., et al. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials, 17*, 2347–2376.
4. Farshid, H. B., et al. (2015). Cloud-assisted data fusion and sensor selection for internet-of-things. *IEEE Journal of Internet of Things, 4*, 1–13.
5. Li, L., et al. (2011). The applications of WiFi-based wireless sensor network in internet of things and smart grid. In *IEEE Conference on Industrial Electronics and Applications* (pp. 789–793)
6. Omer, B. S., et al. (2015). Development of a smart home ontology and the implementation of a semantic sensor network simulator: An internet of things approach. In *IEEE Conference on Collaboration Technologies and Systems (CTS)* (pp. 12–18)
7. Lien, S., & Chen, K. (2011). Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. *IEEE Communications Magazine, 49*, 66–74.
8. Sarkar, S., Chatterjee, S., & Misra, S. (2015). Assessment of the suitability of fog computing in the context of internet of things. *IEEE Transaction on Cloud Computing, pp*, 1–14.
9. Bonomi, F., Milito, R., & Natarajan, P. (2015). Fog computing: A platform for internet of things and analytics. In *A Roadmap for Smart Environments, Studies in Computational Intelligence* (pp. 169–186). New York: Springer.

Chapter 2
Communication Technologies in IoT Networks

Syed Ali Hassan, Sidra Shaheen Syed, and Fatima Hussain

2.1 Introduction

Internet of Things (IoT) has emerged as one of the promising and prominent areas of the 5G communications. As 5G anticipates interconnecting millions of devices around the globe, IoT will be seen as an integral part of various applications such as smart cities, intelligent transportation services, smart grids and many others. Each application area of IoT promises enhanced quality of experience in everyday life activities. For instance, the motivation behind smart cities is to have control over resources, thereby, promoting healthy economy and sustainable growth. To accomplish a successful operation of an IoT era, a network of IoT requires every device to be connected to its utility gateway directly or indirectly. Therefore, these devices are needed to be equipped with smart sensors that collect their data and forward this data to their network operation center for further processing. Many types of IoT networks including centralized and distributed networks have been proposed. However, communications for an IoT network poses an important challenge for its successful operation. Many communication technologies are proposed that can work in conjunction with an IoT network, however, this chapter focuses in detail about a particular form of technology namely the *cooperative communications*, which when utilized in an IoT network promises, large network gains.

S.A. Hassan • S.S. Syed
School of Electrical Engineering and Computer Science (SEEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan
e-mail: ali.hassan@seecs.edu.pk

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_2

In this chapter, various types of IoT sensors and the mode of communication between them are discussed. We also discuss cooperative mode of operation in sensor networks and outlines many topologies that can be utilized. Performance analysis of cooperative communication is also presented to supplement the concepts.

2.2 Types of Sensors used in IoT Network

There are plethora of sensor and actuators that can be used to create various forms of IoT networks. Since this chapter mainly deals with sensor networks and their communication techniques, the following non-exhaustive list of sensors can be used to form homogeneous or heterogeneous networks.

- Machine vision/ optical ambient light sensors
- Acceleration/ tilt sensors
- Position and presence sensors
- Motion, velocity and displacement sensors
- Humidity, temperature and moisture sensors
- Leaks and levels sensors
- Electric and magnetic sensors

A more comprehensive detail of sensor can be found in [1, 2] and references therein. The current and common candidates for communication between these sensor nodes are from mobile communications family including global system for mobile communications (GSM), general packet radio system (GPRS), universal mobile telecommunication system (UMTS)/3G, long term evolution (LTE)/ 4G, satellite communications, licensed or unlicensed radio networks and power line communications (PLC) [3]. These sensor nodes, when transmit or receive data, establish radio links and are therefore termed as IoT nodes or devices in addition to commonly known sensor nodes. The chapter will use these terms interchangeably. The upcoming section presents the transmission strategies on the basis of which these IoT devices communicate with their peer nodes and then the chapter focuses on cooperative method of transmitting or broadcasting data to the entire network.

2.3 Transmission Strategy

The smart IoT devices in a sensor network usually have constraint battery life and operate generally at low transmit powers, therefore, these devices cannot transmit wirelessly to a far-off destination gateway having a direct communication link. Instead, the acquired data is transmitted in a multi-hop fashion to a far-off aggregation point using the intermediate devices as relays. This multi-hopping is performed by the IoT devices that are in a close vicinity to one another. Each IoT sensor device, in cooperation with the devices in its vicinity, relays the data received

from its preceding IoT device(s) to their successor nodes consuming minimal power. This cooperative transmission of data from one set of IoT devices to the next is known as *cooperative communications*. This cooperative transmission phenomenon along with its relaying mode is discussed in the subsequent sub-section.

2.3.1 Cooperative Communications

Cooperative communications is one of the mature domains of modern communication era. The cooperation between IoT devices helps in sustaining the resources of an IoT network. Some of the advantages of this cooperative relaying of information include the increase in diversity thereby increasing reliability, signal-to-noise ratio (SNR), data rates, and hence the increase in the successful hop count or the maximum distance or hops traversed by the information symbols [4]. All these features of cooperative communications are discussed in detail in the subsequent topics of this chapter.

From the past few years, cooperative relaying methods are under consideration of the researchers while developing transmission strategies for inter-device communications. The initial cooperative relaying strategy considered the source destination pair connected via relays in a two-hop manner as shown in Fig. 2.1. However, dense IoT networks with a variety of devices scattered in an area require multi-hop communications for successful data delivery. In cooperative relaying methods, a symbol is transmitted in each time slot. Hence, in conventional strategies, having a single relay between a source-destination pair, the information rate couldn't achieve its maximum limits. These rates were improved by exploiting the channel fading effects and broadcast nature of the wireless channels through diversity.

Multipath fading affects all the wireless channels, causing the variability of received signal level with time and location. In addition to diversity techniques such as temporal, frequency and spatial diversity, a novel idea of achieving diversity is by

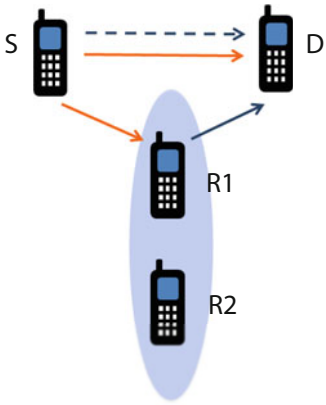

Fig. 2.1 The phenomenon of cooperative relaying. The source node S, uses the help of relays R1 and R2 to deliver the data to the destination node, D. The direct link between S and D may or may not exist. The same information transmitted by relays add the diversity and array gain at the destination, making an overall reliable communication

cooperatively transmitting the information from IoT relaying devices. This improves the chances of correctly receiving the data and minimizes the effect of multipath fading.

The relaying is largely categorized into two types based upon processing of received data. The two major types of relaying are amplify-and-forward (AF) and decode-and-forward (DF).

- Amplify-and-Forward (AF) Relaying: According to AF relaying, the information received at the intermediate IoT device will not be decoded and only the amplified version of the received signal along with noise will be relayed to the successor IoT device(s) of the next hop.
- Decode-and-Forward (DF) Relaying: In DF relaying, the information is relayed to the next set of devices by a preceding IoT device if and only if the data has been correctly decoded by the device. Otherwise, this device will not take part in the cooperative relaying of data towards the destination.

Mostly, the nodes use the DF relaying scheme because of their operation in low SNR regimes, thereby, making an array of devices or hops that remained successful in cooperatively relaying the data.

With all the above inherent advantages of cooperative communication in IoTs, the major issue that this transmission strategy faces is the receive and transmit timing synchronization between the individual IoT devices and the modeling of data propagation. The next sub-section will present the transmission modeling of these cooperative IoT networks by taking into account some possible device arrangements.

2.3.2 Modeling of Cooperative IoT Network

Forwarding or relaying of data packets forming wireless multi-hop communications not only finds its application in sensor and cellular networks but also in mobile computing and wireless computer networks. One such promising technique that also finds its application in the IoT domain is opportunistic large array (OLA) that works on the principle of DF relaying. In OLA, each IoT device decodes the received data and immediately cooperatively relays it to the next set of devices without having any coordination with the devices nearby. This information transverses from hop to hop given that in each hop at least one of the devices decodes the information received from the IoT devices of the previous hop. The set of devices that receives the information at the same time instant forms a hop. In this fashion, the data particularly reaches its destination in an inherent energy efficient manner [4].

There is a possibility that because of the opportunistic nature of communications, none of the devices in a particular hop decodes the information thereby resulting in a killing state. The conditional probability that a node decodes the message, given the message was transmitted before, remains the same for each hop in a given topology, and has paved path for modeling these types of networks by using Markov chains. The decision of successful decoding the data is made on the basis of received SNR being greater than a predefined threshold τ. The range analysis with respect to required SNR margin for the IoT network can be performed by considering the geometry of the nodes, types of channel models and channel impairments.

The propagation of data through an IoT network at physical layer can be modeled by first considering the fixed arrangement of devices along the grid for simplicity. This grid geometry can be one-dimensional (1D) grid geometry and two-dimensional (2D) geometry. In the next subsections, we discuss these topologies and provide performance analysis as to how an IoT network consisting of devices can use cooperative communications to deliver data to a distance destination.

2.3.2.1 1D Linear Arrangement of Nodes in a Network

For modeling of 1D IoT network as explained earlier, the fixed M number of devices can be arranged in a linear grid manner in each hop as shown in Fig. 2.2. Any IoT device in a given level can decode and forward the received message without error given that the received SNR from the previous level or hop is greater than or equal to a threshold. The filled black circles represent the DF devices in each hop. These DF devices from each hop cooperatively transmit the message over the orthogonal channels that can be formed by using orthogonal space-time block codes (OSTBCS). Considering the channel between the nodes to be flat faded Rayleigh, the resultant aggregated power, Y, at a jth node in any hop has a hypo-exponential distribution [5] given as:

$$p_Y(y) = \sum_{k=1}^{K} C_k \lambda_k exp(-\lambda_k y), \tag{2.1}$$

where,

$$C_k = \prod\nolimits_{\varsigma \neq j} \frac{\lambda_\varsigma}{\lambda_\varsigma - \lambda_k},$$

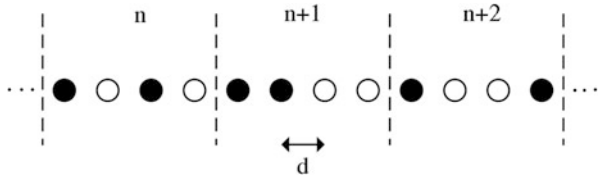

Fig. 2.2 1D arrangement of nodes in a network

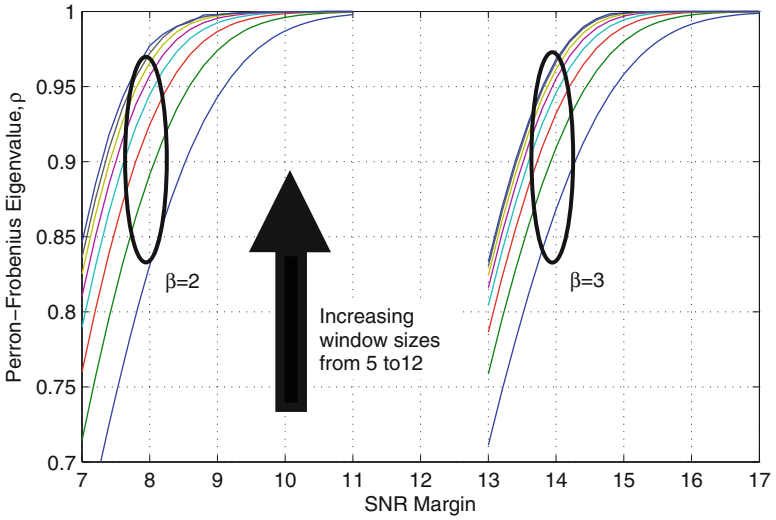

Fig. 2.3 one-hop success probability ρ, which shows the probability that at least one node has decoded and the process of transmission continues

where λ_k is the parameter of exponential distribution, which takes into account the path loss.The probability of successfully decoding a message by a node of the nth hop can then be calculated by integrating the above expression from τ to ∞. This success probability of one node can be used to define the success of a hop and in turn the coverage of the network. In Fig. 2.3, the one-hop success probability, ρ, is shown for different values of required SNR margin, γ. Hence, with the increase in ρ, the probability of successfully decoding a data by different nodes of a hop increases as shown in Fig. 2.3. Also, with the increase in the number of nodes in a hop M, the one-hop success probability, ρ, improves for a given value of SNR margin. The figure also shows that with the increase in the path-loss exponent, β, a higher SNR margin is required for achieving specific success probability.

The performance of the cooperative IoT network versus non-cooperative is depicted in Fig. 2.4 in terms of coverage or the normalized distance an information block transverses for a given quality-of-service (QoS), η. The h_d is the hop count or the percentage of nodes that decodes the data, β is the path-loss exponent, γ is the required SNR margin, and M is the number of nodes in each hop of a cooperative network having fixed boundaries. More importantly, the figure shows that the performance of cooperative case is better than the non-cooperative case for a given SNR margin. The general trend that can be observed is that, with the increase in the number of nodes per hop, M, hop-count h_d increases and so the coverage also increases. Therefore, a large number of IoT devices in a hop can be used for better performance of the overall network.

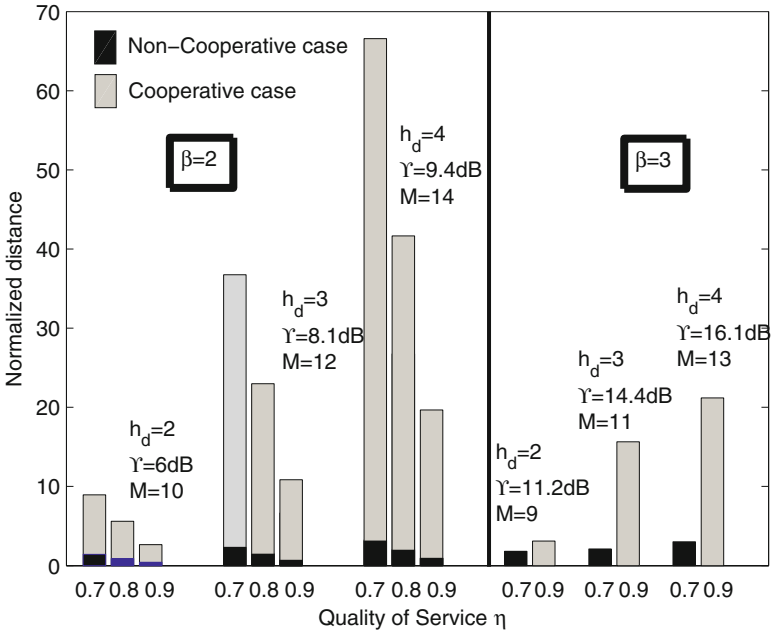

Fig. 2.4 Normalized distance for various cooperative vs. non-cooperative cases

The sensor devices/nodes in a linear cooperative IoT network can also be arranged in a cluster-based co-located manner and its pros over distributed geometry are discussed below.

2.3.2.2 Distributed Versus Cluster-Based Linear IoT Networks

In addition to one-dimensional (1D) arrangement of devices that consists of equally spaced nodes along a line, there is another topology in which the nodes in a hop are placed in a co-located fashion by forming groups along a line as shown in Fig. 2.5.

The major difference between the distributed and co-located topology is that there exists a disparate path loss between the nodes of two hops in case of distributed nodes arrangement. Whereas in case of co-located arrangement, all the nodes of one hop will have same path loss with the nodes of other hop. This same path-loss for the co-located case will result in same exponentially distributed received powers from the nodes of previous hop, i.e. having same λ_k, giving rise to Gamma distribution having PDF as given in (2.2) [6].

$$p_Y(y) = \frac{1}{(|\mathbb{N}n| - 1)!} \tilde{\lambda}^{|\mathbb{N}_n|} y^{(|\mathbb{N}_n|-1)} exp(-\tilde{\lambda} y). \tag{2.2}$$

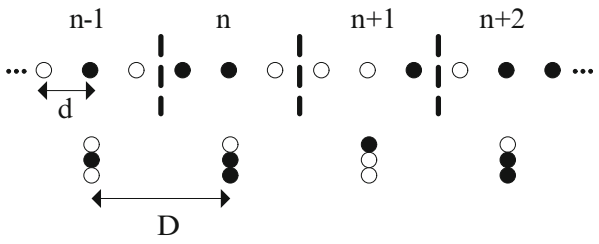

Fig. 2.5 Equi-distant distributed and co-located topologies in line IoT network

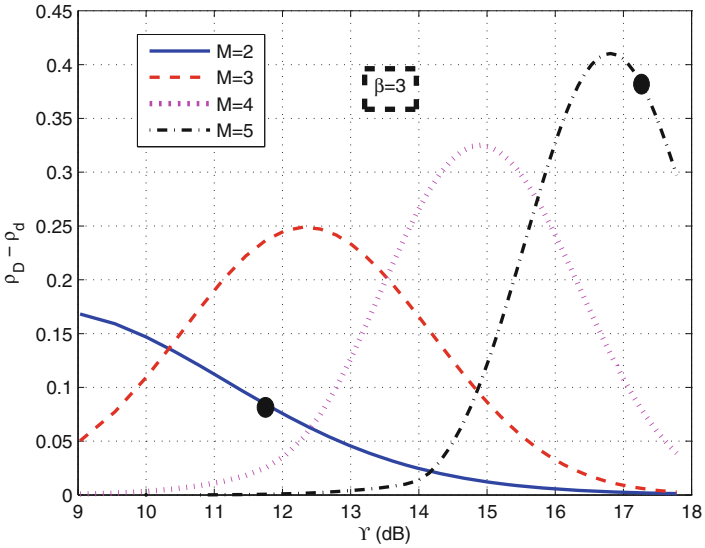

Fig. 2.6 Eigenvalue differences between two topologies; $\beta = 3$

where, $\mathbb{N}_n$ is the set of DF nodes and $|\mathbb{N}_n|$ is the cardinality or length of the DF set. The same path-loss between the node of the two hops accounts for better received power at the jth node of nth hop, and hence results in better one step success probability as shown in Fig. 2.6 for a path-loss exponent of $\beta = 3$.

In Fig. 2.6, the difference between the one-hop success probability of distributed, ρ_d, and co-located, ρ_D, is displayed for different values of SNR margin, γ, and M. The positive difference, i.e., $\rho_D - \rho_d$ shows that the performance of co-located IoT network is better than the distributed IoT linear network, in terms of one-hop success probability, ρ. These results can be extended to a two-dimensional (2D) grid IoT nodes topology, which are presented in the next section of this chapter.

2.3.2.3 2D IoT Network

IoT nodes can either be arranged on the intersection points of a grid and can also be placed randomly along a strip considering strict boundaries in the 2D space. The modeling of the 2D grid-strip is performed in exactly the same manner as of 1D network. But, in case of stochastic node positions along a strip, the distribution of random distance comes into account while examining the performance in terms of energy efficiency and possible obtainable coverage range. The modeling and performance of both of these networks are discussed in the upcoming sub-sections.

2D Grid-Strip IoT Network

The cooperative relaying through these types of networks can take place efficiently on orthogonal channels by employing deterministic orthogonal space-time block codes (OSTBCs) [7, 8]. This implies that the DF nodes of a hop act as virtual multiple-input multiple-output (MIMO) antennas that cooperatively transmit the data block towards the next hop nodes by using OSTBCs. These OSTBCs help in achieving the diversity, reliability, and coverage requirements. This 2D grid-strip geometry having four nodes in each hop is shown in Fig. 2.7.

While using OSTBCs, each node transmits the block of data symbols that makes the one column of OSTBC, whereas, the rows of the OSTBC correspond to multiple time slots. The signal vector received in P time slots at the kth node of nth hop will be [9];

$$\mathbf{y}_{(n)}^{(k)} = P_t \mathscr{G} \left(\mathbf{h}^{(k)} \circ I\,(n-1) \right) + \mathbf{z}, \tag{2.3}$$

where $\mathbf{y}_{(n+1)}^{(k)} \in \mathbb{C}^{P \times 1}$, i.e., $\mathbf{y}_{(n)}^{(k)} = \left[y_1^{(k)} \; y_2^{(k)} \cdots y_T^{(k)} \right]^T$ is the received signal vector at the kth node of the nth hop and P_t is the transmitted power.

The receiver node applies the decoding of the space-time matrix for retrieving the information symbols back. The coverage trend in terms of number of hops

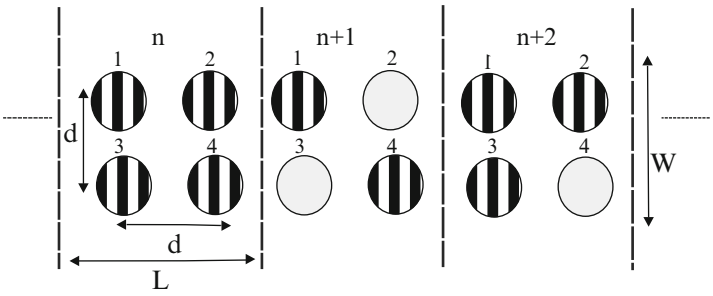

Fig. 2.7 2D grid strip network layout

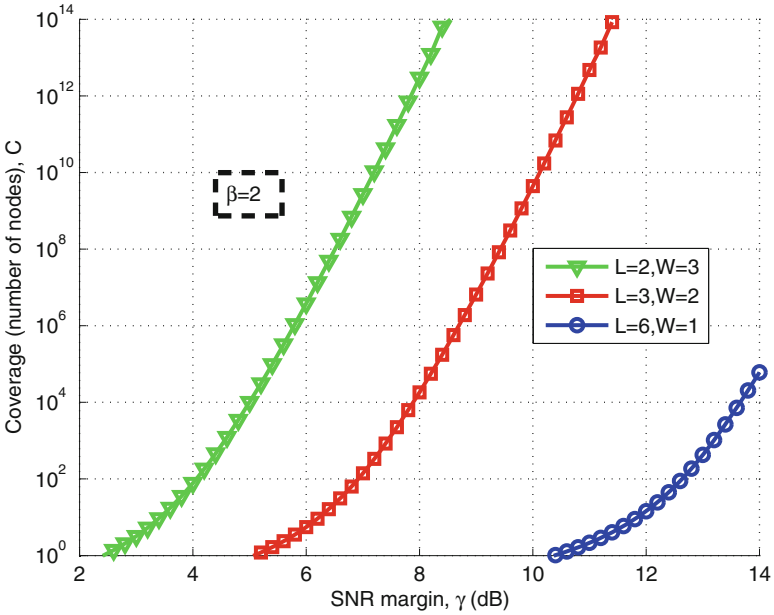

Fig. 2.8 SNR margin vs. maximum coverage for $M = 6$

transversed versus the SNR margin in Fig. 2.8 shows that the 2D topology achieves better performance in terms of one-hop success probability and maximum number of transversed hops as compared to 1D. Here, L and W represent the number of nodes arranged horizontally and vertically in a hop, respectively, where the total number of nodes in a hop is $M = L \times W$. The case where $L > W$ results in smaller coverage as compared to the one in which $L < W$. This is due to the reason that if more nodes are arranged on the horizontal axis then it will result in increased path-loss to the next hop nodes, and hence a degraded performance is achieved.

Stochastic 2D IoT Network

In more practical IoT networks, the node geometry in each hop is considered completely random, i.e., a fixed number of nodes are scattered within a box-shaped hop using a Poisson point process (PPP) as shown in Fig. 2.9. These networks cannot be modeled as a generalization of 1D or 2D grid topologies because of random distance between nodes. This varying distance between the nodes of the two consecutive hops is shown to follow a Weibull distribution [10].

To quantify the coverage, the Weibull analysis is extended to obtain the expression for outage and coverage of this cooperative network with stochastic node positions in [10]. The success probability for stochastic network also increases with the increase in the number of nodes per hop, M. In Fig. 2.10, the contour plot of

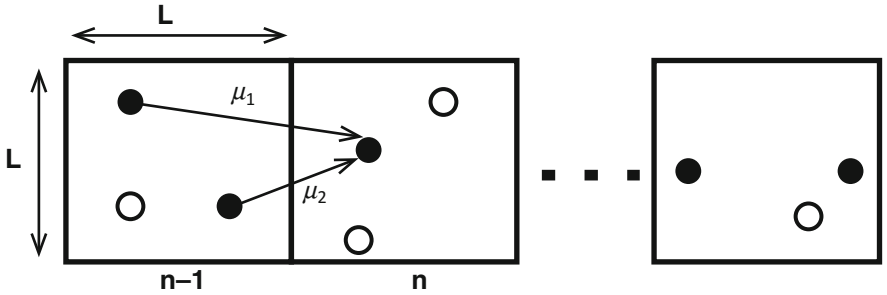

Fig. 2.9 Fixed boundary strip network with randomly placed nodes; $M = 3$

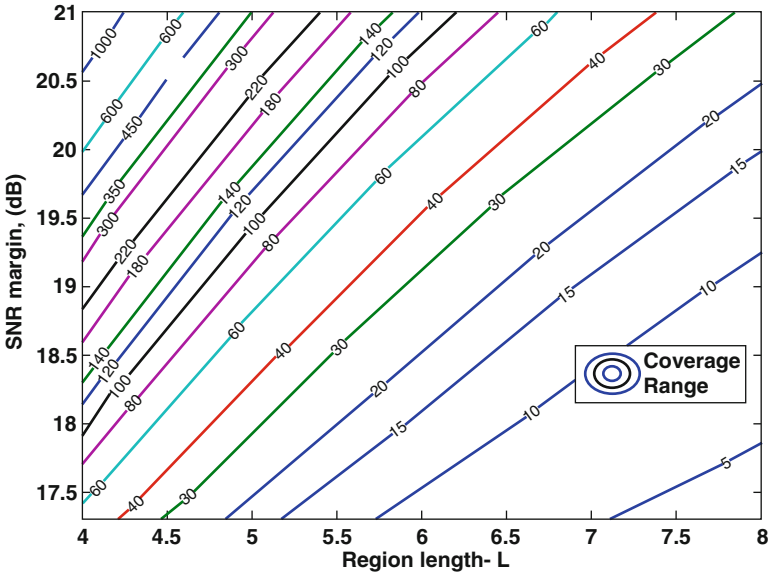

Fig. 2.10 Coverage range for various values of region lengths, L and SNR margin γ; $\eta = 0.8$, $M = 2$

coverage range (CR) against different values of SNR margin, γ, and region length, L, of a hop is shown. For two nodes per hop, i.e. $M = 2$, and a required quality-of-service (QoS) $\eta = 0.8$, the figure shows that with data propagates to larger distances. The reason of less coverage in case of higher region length is that the path-loss is likely to increase with the increase in the area of a hop or its region length L.

For this stochastic geometry, the orthogonal transmission takes place by employing near-orthogonal STBC as used in [11, 12]. These opportunistic networks can be made more energy efficient by having a limited number of nodes to participate in each hop. In this manner, the energy-efficiency of these networks increase, which is an important parameter for an IoT network where the devices generally have low energy values [13].

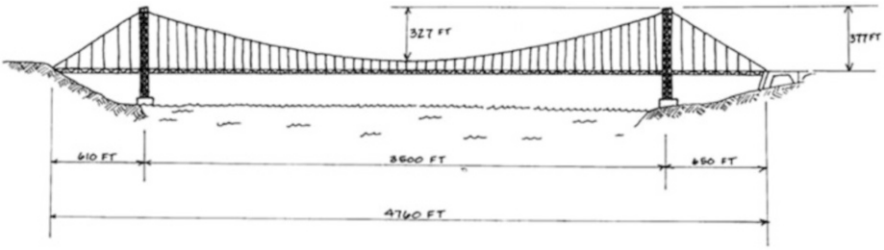

Fig. 2.11 Structural health monitoring of bridges using 1D IoT network

2.3.3 Applications of 1D and 2D Models in IoT Networks

Linear ad-hoc networks or 1D IoT networks find a variety of applications in practical scenarios. Typical examples include structural health monitoring of buildings where the nodes are located in hallways or walls in a linear fashion, however, may not be equally spaced. One-dimensional sensor networks along bridges provide another application area as shown in Fig. 2.11. In this case, a sensor node can transmit its information via cooperative mechanism to a distant central facility. Similar application include fault recognition in transmission lines for future smart grid systems where sensors are installed on transmission lines for their healthy activity. Another important area of application is vehicular ad hoc networks (VANETS), where a spatially random distribution of vehicles is formed along a road with sensors embedded in each of the vehicle.

Strip-shaped networks usually arranged as 2D IoT networks also provide an interesting paradigm of a "plastic communication cable", which is made out of a non-conducting material with embedded radios. Such cables can be used in applications involving high electric fields such as air industry where light materials are required to be mounted on the air vehicles. Similarly, 2D vehicular network where many vehicles are running along a highway constitutes an important application area for 2D cooperative IoT networks.

2.4 Other Candidate Technologies for IoT Networks

Although the focus of this chapter is mainly on a special form of communication technology, i.e., cooperative communications, for an IoT network, however, there are many other techniques which are under consideration or being used in an IoT network which include; millimeter wave (mmWave) technology with or without energy harvesting and interference cancellation. Similarly, many other techniques include spectrum sensing, orthogonal/non-orthogonal multiple access, opportunistic cognitive radio with STBC/distributed beamforming.The existing physical (PHY) layer protocols relevant to IoT are IEEE 802.15.4, IEEE 802.15.6, Bluetooth

Low Energy (BLE), long term evolution-advance (LTE-A), IPV6 over low power wireless personal area networks (6LowPAN), and near field communication (NFC). The main objective of designing communication protocols at lower layers is to achieve high diversity gains, maximize energy and spectral efficiency, and reduce the complexity. Two main approaches in this regard are [14]: techniques for energy-efficient and reliable transceiver design and techniques for low complexity data fusion rules. In addition to (STBC), beamforming technique is employed by considering the distributed nature of sensor/IoT networks where the phase mismatching might affect the performance. In order to make the IoT network more efficient and resilient against collision and retransmission issues, it is required to design estimation/detection techniques having better performance so as to minimize the network overhead [15].

In addition to making the network more energy efficient and reliable by cooperatively transmitting the information, the transmission strategy in [16] also addresses the hidden node issue of wireless sensor networks. To solve the issue of performance degradation due to hidden node problem, various conventional orthogonal and non-orthogonal multiple access (NOMA) techniques are used [17]. As these techniques do not provide a viable solution, therefore, cognitive radio spectrum sensing algorithms can be employed to further mitigate this problem [18].

Moreover, the millimeter wave technology (e.g. E-band) in combination with massive multiple-input multiple-output (MIMO), beamforming and multiple access techniques such as NOMA can ensure significant provide in bandwidth and performance [19] of upcoming IoT networks.

2.5 Summary

This chapter has provided an overview of the types of sensors that can be used in various forms of IoT networks. Further, the transmission strategies through these IoT networks, specially cooperative transmissions, have been discussed in detail, by considering some possible sensor node geometries. Comparative results for coverage of each topology have been provided with an in-depth analysis. It can be concluded that cooperative mechanism provides an elegant and simple strategy to obtain reliability in future IoT networks, which is an integral demand of 5G communications. Towards the end, the chapter is concluded by mentioning some of the other candidates of communication techniques used in IoT networks in addition to cooperative communications.

References

1. Kim, H. Y. (2016). A study of a smart IT convergence framework in IoT. In *Proceedings of the 9th International Conference on Security of Information and Networks, ACM* (pp. 174–175).
2. Kelly, S. D. T., Suryadevara, N. K., & Mukhopadhyay, S. C. (2013). Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE Sensors Journal, 13*, 3846–3853.
3. Liposcak, Z., & Boskovic, M. (2013). Survey of smart metering communication technologies. In *IEEE EUROCON* (pp. 1391–1400).
4. Scaglione, A., & Hong, Y. (2003). Opportunistic large arrays: Cooperative trans-mission in wireless multi-hop ad hoc networks to reach far distances. *IEEE Transactions on Signal Processing, 51*(8), 2082–2092.
5. Hassan, S. A., & Ingram, M. A. (2011). A quasi-stationary Markov chain model of a cooperative multi-hop linear network. *IEEE Transactions on Wireless Communications, 10*(7), 2306–2315.
6. Hassan, S. A., & Ingram, M. A. (2012). Benefit of co-locating groups of nodes in cooperative line networks. *IEEE Communications Letters, 16*(2), 234–237.
7. Alamouti, S. M. (1998). A simple transmitter diversity scheme for wireless communications. *IEEE Journal on Selected Areas in Communications, 16*(10), 1451–1458.
8. Tarokh, V., Jafarkhani, H., & Calderbank, A. R. (1999). Space-time block codes from orthogonal designs. *IEEE Transactions on Information Theory, 45*(7), 1456–1467.
9. Syed, S. S., & Hassan, S. A. (2014). On the use of space-time bock codes for opportunistic large array network. In *IEEE Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1075–1080).
10. Afzal, A., & Hassan, S. A. (2014). Stochastic modeling of cooperative multi-Hop strip networks with fixed hop boundaries. *IEEE Transactions on Wireless Communications, 13*(8), 4146–4155.
11. Sirkeci-Mergen, B., & Scaglione, A. (2007). Randomized distributed space-time coding for distributed cooperative communications. *IEEE Transactions on Signal Processing, 55*(10), 5003–5017.
12. Syed, S. S., Hassan, S. A., & Ali, S. (2015). Near-orthogonal randomized space-time block codes for multi-hop cooperative networks. *IEEE Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 840–845).
13. Ansari, R. I., & Hassan, S. A. (2014). Opportunistic large array with limited participation: An energy-efficient cooperative multi-hop network. In *IEEE International Conference on Computing, Networking and Communications (ICNC)* (pp. 831–835).
14. Kim, T., et. al., (2015). Physical layer and medium access control design in energy efficient sensor networks. *IEEE Transactions on Industrial Informatics, 11*(1), 2–15.
15. Cui, S., Goldsmith, A. J., & Bahai, A. (2005). Energy-constrained modulation optimization. *IEEE Transactions on Wireless Communications, 4*(5), 2349–2360.
16. Wang, W., & Lau, V. K. N. (2014). Delay-aware cross-layer design for device-to-device communications in future cellular systems. *IEEE Communications Magazine, 52*(6), 133–139.
17. Blum, J., & Eskandarian, A. (2013). A reliable link-layer protocol for robust and scalable intervehicle communications. *IEEE Transactions on Intelligent Transportation Systems, 8*(1), 413.
18. Aijaz, A., & Aghvami, A. H. (2015). Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. *IEEE Internet of Things Journal, 2*(2), 103–112.
19. Pi, Z., & Khan, F. (2011). An introduction to millimeter-wave mobile broadband systems. *IEEE Communications Magazine, 49*, 101–107.

Chapter 3
Big Data and Fog Computing

Fatima Hussain and Ameera Al-Karkhi

3.1 Introduction

Internet of things (IoT) is considered as an interconnected complicated network of people, machines, and smart things. An important feature of the vision of IoT is defined as: observation of behavior of "smart things" will make possible to gain important insights, and resulting process optimization. Common outcome of this emerging IoT field is the creation of large amount of data, and as a result its storage, expiry and ownership raises many critical issues. This stored data has to be used intelligently for smart monitoring and actuation. Centralized and distributed artificial intelligence algorithms are required for automated decision making after smart sensing/monitoring. In addition to this, state of the art machine learning and data fusion algorithms are required to infer or extract useful information from stored data. This vision leads to solve multiple challenges like:

- weather or not to store all the events
- to run analytical queries over the stored events
- to perform analytic (data mining and machine learning) over the data to gain insights

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

A. Al-Karkhi
Ryerson University, Toronto, Canada
e-mail: a.a.alkarkhi@gmail.com

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_3

It is believed that anything that has capability of connecting, will be connected and can communicate through wireless sensors or RFIDs or similar devices. These things will be communicating and sharing immense amount of data among each other and with people as well. This raw data is and need to be classified and organised according to the application requirement. This gathered data is given the name of "Big Data", as it has high volume and immense variety of information, and require high processing speed. It demands not only cost effective processing, but also unique automation of resulting data. Cloud computing platform is used to serve all these requirements, in general. We can define this Big Data with three basic characteristics, as below.

Variety of data information means that, IoT data is diverse in nature, may be structured or unstructured with diverse data models, types, formats and query languages, and from diverse data sources.

Volume of data is huge and requires ware-houses with big data storage capabilities.

Velocity of data generation is fast and inherits high speed of data flow and requires efficient data processing analytic.

One of the most prominent features of IoT is its real time or near real time communication of information about the "connected things". This becomes more challenging when this is done on a large scale. In addition to this, smart applications and scenarios, in many cases, are also characterized based on the variety of data sources and pose challenges for their storage and processing. Many IoT applications are distributed over large geographical area and are delay constrained, and require efficient data storage and processing techniques. All of these challenges faced by cloud computing due to special requirements of most of IoT applications, are further discussed in detail in the following. Restricted or rather unsatisfactory performance of cloud computing enables us to move to fog computing platform [1].

Fog computing is considered as an specialised extension of cloud computing, which brings few of the important processes near the user end and keep the rest in cloud. This computing system is becoming popular specifically, for real time and latency sensitive IoT applications. Fog uses the same storage, networking and computing resources as cloud and share most of the similar attributes [2].

In this chapter, we discuss about big data generated from IoT networks, and corresponding challenges. We also discuss suitability of cloud and Fog computing for specific IoT applications. Afterwards, we present a use case for smart parking system and discus the suitability of Fog platform for this scenario.

3.2 Data Analysis

IoT services are comprised of three basic functions: data sensing and collection by smart devices, analysis of this data, and device automation based on this analysis. This analysis can be massive real time deep analysis. Broadly speaking, we can divide data analysis into three categories.

Massive data analysis is required as data is collected from many devices and sensors, and huge amount of data is stored and accumulated in database.

Real time data analysis and continuous processing is required to analyze data generated from various smart devices with higher data rates.

Deep data analysis is required for forecast of power consumption, failure prediction and pointer to specific data point.

3.2.1 IoT Data Analysis Challenges

IoT is a network of everyday objects (anything, everywhere and anytime). Identifying and networking all the objects in the world establishes a new paradigm of digital interactions with the physical world; presenting a revolutionary transformation in our daily lives [3]. With the recent advancement of smart computing environments, IoT paradigm has become an integral part of many aspects of our daily lives from connected homes and cities to connected cars and roads to devices that could follow individual's behavior [4]. However, people have limited time, attention and accuracy, which means that they are not so conscious and good at capturing data about things in the real world. Therefore, the emergence of embedded computers and smart sensor networks that can gather information from the environment of things to provide ubiquitous access to various data to people at lower costs without loss of time [5, 6]. In the following sections, a number of IoT data analysis challenges are discussed such as data security that has to be ensured to protect the integrity of the system, data collection, data analytic and communication protocol standardization challenges. Those issues require research on new types of data analysis methods.

3.2.1.1 Security Challenge

In IoT environments, users expect to access resources and services anytime and anywhere, leading to different and more serious types of security risks. Such environments also pose different types of access control problems as their resources are now more accessible to more people and by a wide range of machines. A network inside such environment is expected to dynamically connect to other networks and change its topology, and hence will require more complex access control. For example, when mobile devices join and leave a certain mobile zone, and as their wireless short range radio interface goes in and out of range of access points or other mobile devices' reach, using a traditional technique like firewall will be inadequate because we need a firewall to protect each of the devices [7]. In recent world of networking and computing, there is no problem protecting systems, and security can be implemented by using firewalls or intrusion detection systems to separate trusted and un-trusted parties in a network. However, in IoT these techniques are unusable and unworkable, especially when considering the case of a device stolen or lost, which is a new case in the recent world of networking.

Pervasive computing can be divided into two main groups. The first group is personal devices which are usually carried by individuals. The second group is infrastructure devices which are embedded in the environment [8]. The interaction between these two categories declares the need for a new security model. Therefore, suitable security model for IoT networks will not be achieved by forbidding everything; but by "monitoring, evidence gathering and reconciliation". There is a need to build a new framework, which includes a technical security solution, services and rules for good behaviour and ways of dealing with pervasive computing security breaches.

User authentication and access control strategies can be used to provide security in small networks and stand alone computers. These strategies are used to verify the identity of a person or a process in order to enable/restrict the ability to change, use, or view resources. However, the wider development and flexibility in distributed networks, such as the Internet and pervasive computing environments, show that these strategies are inadequate, because such systems lack central control and their users are not all predetermined, leading to serious risks and access control problems.

Consequently, security is a crucial design issue in IoT (because of the usability and expansion of IoT applications) which depends on the security and reliability provided by the applications [9]. In such an environment, there is a strong possibility that people will be monitored by a large number of invisible computers, either private or public. Therefore, designer of these systems should understand how people can trust such an environment and then can accept it. Furthermore, IoT environments should consider other security issues such as privacy, trust, and identity. Because of the wider interaction between the IoT and people, privacy becomes particularly important as people learn about the existence of such systems and become protective of their own privacy. This is because they do not know how their personal data is collected and what the purpose behind this is. Therefore,

many researchers suggest different ways such as anonymity to protect the users' privacy and give the right to users to choose whether to distribute and exchange their personal data or not.

Two other security issues linked to privacy are trust and identity. Whenever a user trusts a system, he or she will be more inclined to reveal their personal data. Because of the dynamic connections between the device and user, the user will depend on the trust relationship agreed between them. Establishing user identity in pervasive computing environments requires special attention, because using the traditional security techniques will be insufficient to establish and verify the identity of users. This is due to the mobility of the devices and the random connection between devices and users. Thus, providing a method to verify the real identity of a user will be necessary for the success of such environment. Moreover, it is important to note that pervasive computing environments require a new type of authentication (called authentication of artifacts), which means a physical artifact has to prove that it knows a secret, in addition to the need for other traditional types of authentication [10].

3.2.1.2 Privacy Challenge

In IoT environments, where the concentrations of "invisible" computing devices are continuously gathering personal data and deriving user context, the user should rightly be concerned with their privacy. Devices may reveal and exchange personal information (such as identity, preferences, role, etc) between smart artifacts in such systems. In a context where devices cannot be assumed to belong to a single trusted domain, privacy becomes a major issue. It is crucial to develop and create privacy-sensitive services in IoT systems to maximize the real benefit of such technologies and reduce feasible and actual risks. Because such systems collect a huge amount of personal information (such as e-mail address, location, shopping history etc.) and because people are typically concerned about their personal information, it is conceivable that they will be reluctant to participate in IoT environments. Thus, it is important to provide a mechanism that ensures privacy is maintained at all times. Privacy can be defined, as "an entity's ability to control the availability and exposure of information about itself". There are five characteristics that make such systems very different from today's data collection systems, which are:

- new coverage of smart environments and objects will be presented everywhere in our life
- data collection will be invisible and unnoticeable
- the collected data will be more intimate than ever before; for example how do people feel while doing something

(continued)

- the underlying motivation behind the data collection
- the increasing interconnecting which is necessary for smart devices to cooperate in order to provide a service to users; this results in a new level of data sharing making unwanted information flows much more possible

Together, these characteristics indicate that data collection in the age of IoT is not only a quantitative change from today, but also a qualitative change. Users in IoT environments do not know what is done with their personal information and a service may store or process the provided data in some way that is not intended by the user. This fear makes people feel more concerned about their privacy. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used and what are the consequences of any given action.

We can refer to privacy as a solution research issue; it has always been raised as a crucial issue for the long-term success of pervasive computing. The concept of privacy has become one of the main concerns as the technology of smart artifacts develops. Moreover, in the developed world there has also been a growing awareness of privacy issues in general, particularly due to the increased use of the world wide web. A well-designed pervasive system can eliminate the need for giving out some items of personal information. For example, schemes based on "digital pseudonyms" could eliminate the need to give out items of personal information that are routinely entrusted to the network's today, such as credit card number and address.

3.2.1.3 Data Collection Challenge

The data acquisition challenge represents the information collection unit and could include a huge number of heterogeneous and distributed sensor types such as, sensed context (physical or software sensors), interaction or control sensors. Such information could be noisy and incomplete for metadata due to noise or sensor failure. It is important to figure out, how intelligently we can transmit only necessary and meaningful data. It will result in a clean analytic without processing junk data.

One of the method used for this purpose is activity recognition system which has the ability to monitor user activities in smart home environments [11]. User activities can be monitored via processing data coming from various sensors. As a result of user interactions with various devices and sensors, the amount of generated information can be very large and managing it will be a challenge. Therefore, a multi-level hierarchical activity inference process, which is distributed, can be used. It supports the notion of self-organizing of various object networks structure. The object network structure has the duty of allowing the processing of low-level information, which comes from primitive sensors, by recursively composing the low-level

information into high-level abstraction. Then the information flows to a decision module that matches this data in the user activity map to finally infer user activity.

Cloud computing is suggested for such type of data collection and abstraction challenges. It is different from the other computing concepts in having the feature of the abstraction of resources.

Cloud computing is defined as the delivery of services through configurable computing resources over the internet.

Cloud computing definition is built on five essential characteristics [12]:

- on-demand self-service
- resource pooling
- broad network access
- rapid elasticity
- measured service

Cloud computing provides benefits to both the providers and users. For the providers' side, it enhances the computing power and the storage capacity, whereas, for the users' side, it provides and guarantees them with the requested resources seamlessly for less cost. Users in cloud computing use various devices (for example, laptops, smart phone) to gain access to storage or application-development platforms using services offered by cloud computing providers. Furthermore, by utilizing the power of the cloud computing in terms of elasticity, storage loads, and scalability, context processing and service delivery could be improved to provide the user with better and cheaper services delivery.

3.2.1.4 Data Analytic Challenge

As IoT is aiming for autonomous and smart behavior, applying analytic tools or kind of correlation techniques is a vital challenge. This challenge is more related to filtering the entire analytic process. The issue is: where it can be possible to do all these analytic? It could be that some part can be performed within the devices, so that the data coming out of these devices are filtered to some extent. Or, we could design separate analytic layers once the data is collected unchanged, and then perform the filtration step by step. Finally, do the analytic with the clean data.

Cloud computing can provide the extra processing and analysis incurred from managing the collected information. We believe that building an application such as an intelligent middleware (using machine learning tools or data mining) that acts as a bridge between the operating system and an application(s) could solve the big

data analytic issue. This is in addition to apply a proper strategy that has to be built to figure out how the storage and analytic can be managed.

3.3 Internet of Things: Data Management and Processing

3.3.1 IoT Requirements and Cloud Computing

IoT network is known as cyber physical and social systems, as it is comprised of smart machines with diverse characteristics and social networks of humans. It facilitates human to human (H2H), human to machine (H2M) and machine to machine (M2M) communications. Few application scenarios include smart transportation, smart city, smart grids etc. For these applications to work, high transmission rate, reliability and energy efficiency must be maintained [8]. Efficient network architecture is required in addition to the improvement in air interface for these kinds of networks.

Most of the user generated data for IoT networks is comprised of pictures, documents and videos, and is generated at the user edge. Consequently, presently adopted network architecture of layers is not able to handle these heterogenous systems efficiently. By appreciating various challenges foreseen for the deployment of IoT networks, we conclude that conventional cloud computing architecture will not be feasible to use. Also, cloud architecture is centralised in nature, therefore, cannot satisfy delay constrained and real time IoT devices at user ends. In fact, virtualisation of services in clouds is the reason behind its unsuitability for most of the IoT applications. High latency is introduced in service provisioning in cloud architecture due to services stored in geo-spatially remote locations. All of these technological requirements for IoT data and inability of cloud to handle most of the IoT applications, calls for the evolving state of the art computational paradigm [13].

The Fog vision is conceived to address applications and services that do not fit well in the paradigm of the cloud [14]. These can be listed as under:

- Applications which require low latency such as gaming and video conferencing.
- Applications which are distributed over the large geographic areas such as environment monitoring WSN, connected rail and smart traffic etc.
- Fast and mobile applications such as smart connected vehicle and intelligent transport system etc.

3.3.2 Fog Computing Architecture

Fog was first proposed by Cisco, and they called this new computational platform as fog. They wanted to develop an companion platform for cloud by moving few functions to the network edge, from core of the cloud [14]. It is not used as substitute for cloud rather used to overcome its shortcomings. Complimentary companionship

of fog and cloud will enable low latency IoT tasks to run at user end, and complex time consuming computational task and analysis at the core network.

3.3.2.1 Fog Attributes

Prominent attributes of fog is the de-centralized management and cooperation [13]. It is comprised of a large number of interconnected smart devices and capable of forming many mini clouds. These mini clouds are formed at the edge of the network and are distributive in nature. Fog computing enables processing/computing tasks at the user edge, contrary to cloud. Tasks are distributed between fog and cloud, only those tasks not handled well by edge systems are taken to the cloud. As a result, computing and routing burdens are significantly decreased thus improving the efficiency. It also adds to scalability and lowers network traffic. For example, fog can be used by the end users to store and fetch data instead of cloud. This data is closer to users and therefore end to end latency is improved. Self driving vehicles and wearable devices are few to name, which can benefit from fog computing.

3.3.2.2 Interplay of Cloud and Fog

Collectively speaking, IoT requires an efficient storage, computing and networking resources to/from the user end to the cloud center. Many applications require an collaborative interplay between the edge and the core of the network. As data generated and stored from various smart devices has different requirements at different time scale, it demands active cooperation between the user end and the cloud core. Smart vehicles and smart parking are few to mention, and require hierarchial organisation of resources and computing between fog and cloud.

3.3.3 Context Awareness in Cloud and Fog

Using cloud/fog computing and context-aware systems could help in solving and executing complex tasks. It can provide highly scaled and distributed services in terms of computing power, storage and memory as needed.

It is essential to highlight the meaning of awareness in cloud/fog for IoT applications, as it is different from the pervasive computing sense. It is not about the human but about the smart devices, which means the collected information of awareness has to be personalized and customized. Moreover, with the widespread use of different smart devices like smart phones, tablets (which can be mobile); require services to tailor their context and cope with the issues of context delivery and services selection. The idea of incorporating context in fog and cloud computing will help in gaining better understanding and representation of this smart computing environments.

Most widely used context indicators are location, time, temperature, pressure, humidity and neighbour changes. Researchers considered four context dimensions to setup context information; time, location, social settings (e.g., a set of devices/humans working on one or more application that depends on one another) and object's present (like applications running).

Challenges in context-aware are; collection and aggregation of the context information in a structural manner, and choice of situation context services for context delivery to devices [12]. There is a requirement of framework for context provisioning, in order to cope with context delivery and context services selection. Authors in [12], proposed such a framework based on context brokers, who work as a mediator between the context consumers and the context services. These are the premature form of foglets and are using a publish/subscribe model for their operation. In addition to this, another model was proposed by [15], for improvement of quality of service. Authors combined the techniques of context awareness and adaptive job scheduling, and was able to rationalize the resource utilization. As a result resource wastage is reduced by scheduling the jobs according to the changes in device's context.

Device/human context information can be used to define priorities of tasks executed in the cloud/fog associated with the applications running on the smart portable device. Therefore, context monitor is required to collect and interpret contextual information followed by storing and indexing in the database. Afterwards, end-user context information and configuration parameters are used to translate context information to task priorities. In addition to this, inferring the context distance between events received from the environment and system's situation is also important. This distance is recorded using context analyzer and is used to arrange the status of available tasks.

The main goal of the area of context-aware cloud/fog computing is to collect information about the device/human and the surrounded environment by utilizing the smart device, and network services, which are embedded in an environment. Each smart device is capable of gathering broad context and social information such as the availability of remote resources, network bandwidth and weather conditions from their surrounding environment. Below we mention some of the promising benefits of combining context in cloud/fog computing:

- will support spontaneous applications provisioning.
- devices will have awareness about the context.
- access to remote information and services.
- system adaptability can be achieved according to human/device profiles and context information.
- context will enable a new generation of interesting smart applications that are personalized to one's location, activities, preferences, and friendship relationships.

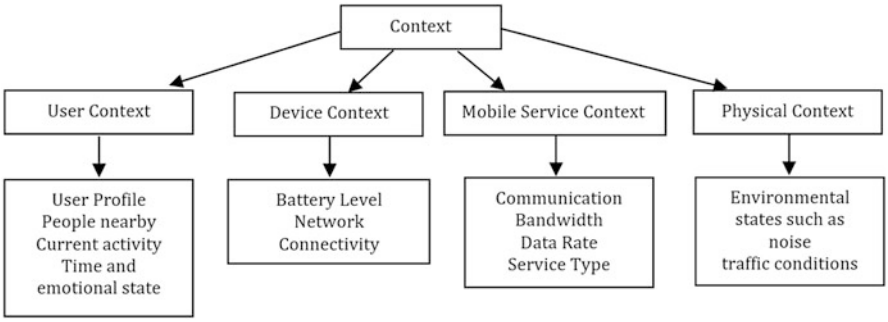

Fig. 3.1 Context categories in cloud/fog computing

- optimization of context communication and coordination between smart devices and the cloud services, in order to conserve energy.

We conclude that context in cloud/fog computing is mainly divided into four categories and Fig. 3.1 shows these different context categories:

> User context consists of the user's profile, people nearby, current activity (meeting, driving), location (GPS or IP address if WiFi is connected), time and emotional state. Device context includes the battery level (for example when it is low battery the screen bright goes dimmer through sensing the photo sensor). Mobile service context includes the network connectivity, communication bandwidth, data rate, service type (cellular 3G/WiFi). Physical context comprises of the environmental states like the noise level, traffic conditions, and temperature.

3.3.4 Internet of Things and Cloud/Fog Use Case

In the following, we elaborate the benefit of fog and cloud interplay by considering context awareness. We use this framework later in designing the model for smart parking system.

3.3.4.1 Integrated Cloud and Fog Based Context Aware Framework

A sample of context-aware cloud/fog computing framework is presented in Fig. 3.2. It is based on designing a middleware responsible for retrieving raw data, abstracting and merging the sensed data into high level context, then making it generic

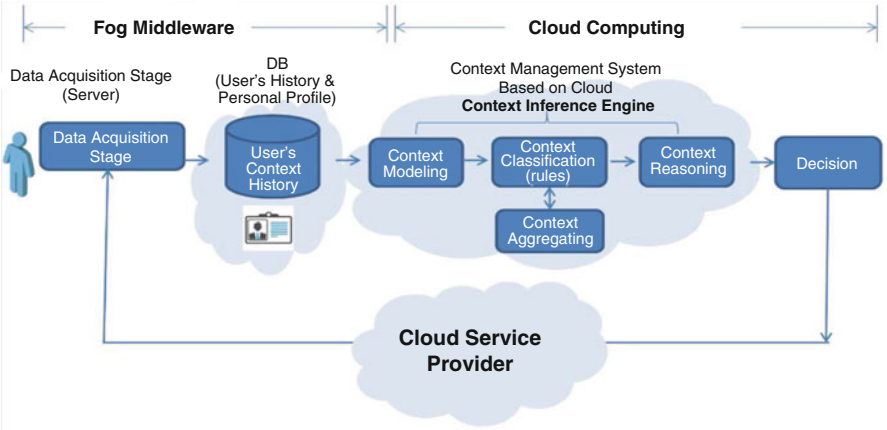

Fig. 3.2 Fog and cloud based context-aware system framework

for different context-aware applications in cloud computing. This middle-ware represents the fog computing that facilitates computing directly at the edge of the network and can deliver new applications and services especially for the future of internet.

> The fog computing characteristics, such as low latency and location awareness, geographical distribution, mobility and huge number of nodes, make the fog the most appropriate platform for IoT services and applications like smart cities and connected vehicles.

Implementing such a framework can help in targeting robust and highly scalable and appropriate cloud/fog computing applications. It could be one of the tools that facilitates development of components and how to fit different components together. This framework offers monitoring, collecting, and processing of user's context and environmental data. It incorporates machine intelligence to generate a decision to the device/user. The implementation requires reconfigurable storage to handle user context information, in addition to high computing and processing power. Adding fog and cloud computing has various advantages such as providing sensor data management and remote monitoring services, ubiquitous storage and scalable computing capability while maintaining an economical budget and computing power on demand. In addition, it will improve the quality of services and reduce the cost.

Figure 3.2 depicts the abstract architecture of the proposed middle-ware. The data acquisition stage represents the context collection unit and could include a number of heterogeneous and distributed sensor types such as, sensed context (physical or software sensors), interaction or control sensors. The fog database stage represents the user's knowledge base component which include the user's

profile and context history. The context management system that is in the cloud side, includes four components: context modelling, context classification, context aggregation and context reasoning. The context management system is responsible for several functions such as, managing and storing user's context, mapping the suitable service for a specific user's context in addition to managing the access control to the user's information and history.

3.3.4.2 Smart Parking System: A Use Case

Intelligent parking spot detection is emerging as a topic of increasing research importance, as real time parking detection leads to savings in time and fuel mainly in urban areas. Convergence of IoT networks and smart phone applications help the deployment of smart parking systems. Smart parking can help drivers to be informed in real time about the availability of vacant parking spots. We propose the usage of foglets to address the problem of street parking and intend to develop an IoT based prototype. Our proposed system not only locates the empty parking spots in current time but also identifies potential empty spots in the near future. It constructs each parking spot as an IoT network, and foglets are used for local processing and storage. Data including parked vehicle locations, parking time duration and current and potential empty spots in road side park areas, is stored in fog devices. We use cameras to capture wide angle images and integrate this information with ticket machine data. Cameras can record and detect parking spots' real time information on road sides and transmit to foglets, used as an operational unit for processing information from cameras and ticketing machine database. This parking information is displayed on boards and also can be accessed through smart phones. Given the fact that not all drivers carry a mobile phone and the fact that not all drivers with a mobile phone have the smart parking system installed, our system can still provide assistance on availability of street parking spaces.

Definition 1 Foglets are defined as fog agents near user ends, having software/hardware modules, and capable of data storing, processing and automation.

We propose fusion (in fog) of ticket machine data fetched from a city database (cloud), and real time camera images (in fog) to predict vacant parking spot. We utilize camera images in our proposed architecture and store/receive this data to/from the city data base cloud in real time. Doing this for each driver is not very efficient. Therefore, we use foglets to efficiently store and process multimedia data. Our fog device possesses limited semi-permanent storage that allow temporary data storage and processing for the real time queries from car parking drivers. It is not efficient to perform data queries every time from the ticket machine database, as it will result into unnecessary increase in network traffic and latency. We have distributed vacant spot search functions, into foglet and ticket machine database modules. The foglet is responsible for information extraction from camera images and also for processing this data to locate empty spots in current time. If there is no empty spot available at the current time, then foglet will process the ticketing

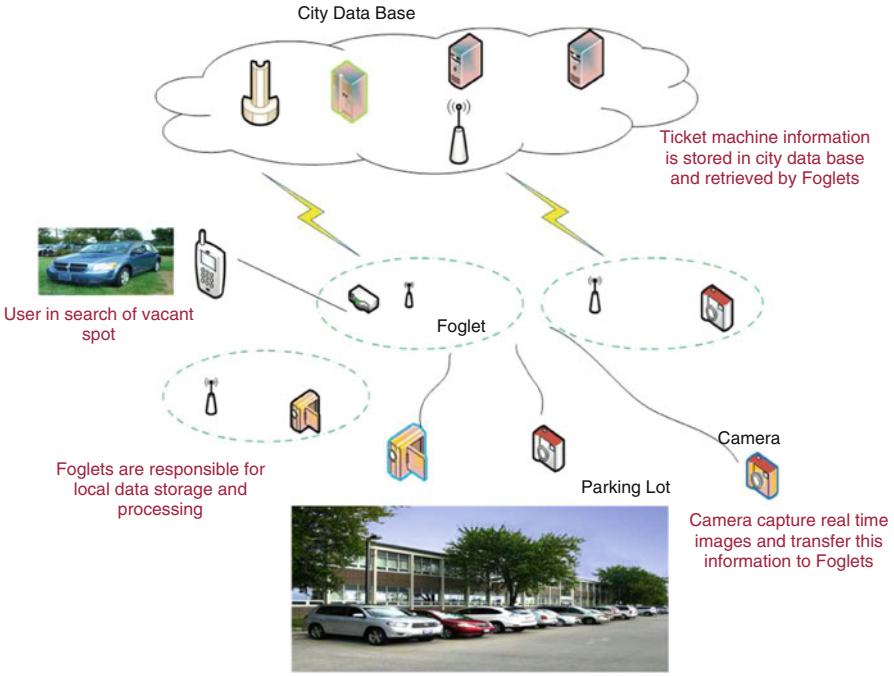

Fig. 3.3 System architecture for road side smart parking

information after fetching reservations from the city data base. This way, drivers will be informed of spots that are most likely going to be vacant in future time; perhaps such as in 5 min or 10 min. The foglet is also responsible to access the data base in an efficient and controlled manner, trying to reduce the power consumption and latency by eliminating communication directly between city data base and driver. Figure 3.3 shows the proposed system architecture.

Proposed Model

Let S_n^v be the number of vacant spots, and S_n^f be the spots currently occupied and being available in the near future. Each driver M is informed of S_n^v and S_n^f, and hence available spots S_n^a to each driver is given as:

$$S_n^a = S_n^v + S_n^f, \forall S \tag{3.1}$$

Let C be the overall cost of parking search, $C(P)$ and $C(L)$ be the cost due to power consumption and latency, respectively. We introduce a binary variable $u_{x,y}$ describing the parking action of a user such that, $x = 0 \rightarrow M$ and $y = 0 \rightarrow M$, where x and y denotes the current and future vacant spots, respectively.

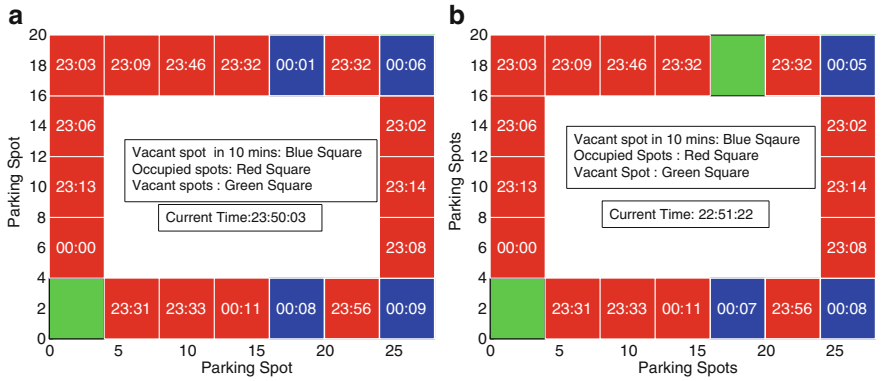

Fig. 3.4 Parking status in 10 min time duration. (**a**) Parking status at t_1. (**b**) Parking status at t_2 after 1 min

$$u_{x,y} = \begin{cases} 1 & \text{if user park at } S^v, \\ 1 & \text{if user park at } S^f, \\ 0 & \text{user does not park,} \end{cases} \tag{3.2}$$

where S^v and S^f (Eq. (3.1)) are current and future available spots, respectively. We want to minimize the cost of finding vacant spot and is formulated as:

$$\Phi = min \sum_{x=0}^{M} \sum_{y=0}^{M} (C_{x,y}(P) + C_{x,y}(L)) \tag{3.3}$$

Such that:

$$\begin{cases} \sum_{x=1}^{S^v} u_{x,y} \leq 1, \ \forall x, y, \\ \sum_{x=y}^{S^f} u_{x,y} = 1, \ \forall x, y \end{cases} \tag{3.4}$$

where M is the total parking spots in all the sides of a building. $\sum_{x=1}^{S^v} u_{x,y} \leq 1$ indicates that each user may find and is able to park at most in one vacant spot. In our proposed system if a user is not able to find any vacant spot on arrival, he is still able to find vacant spots in the near future as described by $\sum_{x=y}^{S^f} u_{x,y} = 1$.

Time Prediction

In Fig. 3.4, spots that will be vacant within 10 min are shown. Drivers near the building are interested in vacant spots or spots going to be vacant in 5, 10 min time. Foglets will do the data and image processing and can display information about spots that will be vacant in any given time. We can see at t_1, the top side's

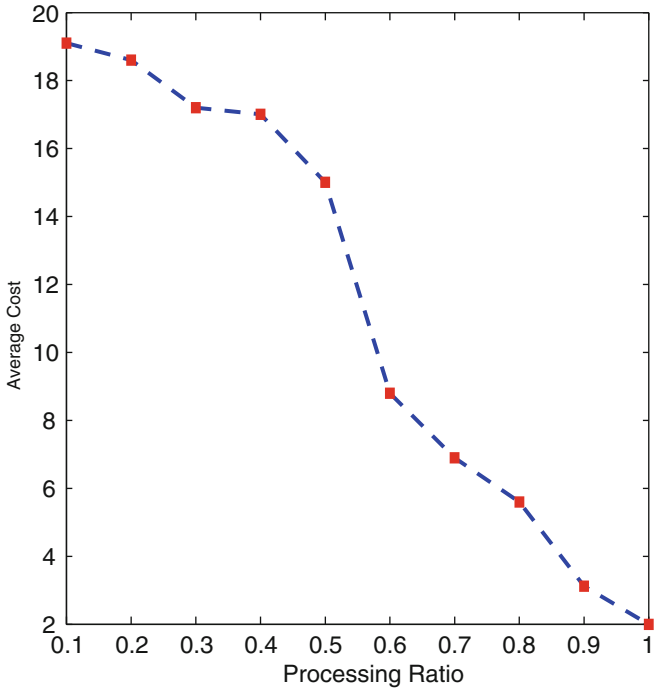

Fig. 3.5 Average cost versus processing ratio

third parking spot from right is going to be vacant in 1 min and is shown by a blue square, as shown in Fig. 3.4a. While Fig. 3.4b shows the status of parking lot at t_2 after 1 min and we see that same spot is shown by a green square. If the driver does not vacate the spot after reserved time is expired, camera images in real time further compliment the results accuracy. In addition, occupied but expired spot information can be queried by parking enforcement authorities for further action. Data fusion and processing between this predicted vacant spot and images taken by cameras at the current time are done in foglets.

Cost Minimization

In Fig. 3.5, decrease in the cost function is shown when our proposed system is implemented. We take cumulative effects of $C_{x,y}(P)$ and $C_{x,y}(L)$ and plot against the ratio of local to centralized processing. We name this ratio as cost improvement Ψ. We take the cost of local processing as to be 3 units and of centralized processing as 20 units [1, 2] and plot the average value. We see that as Ψ increases, cost decreases. This was expected as more of the processing is done at foglets, and less use is made of city data base, which is the expected benefit of doing fog computing. This results

in the reduction of processing and communication time. It also reduces the power consumption at the central database. Here we have shown the cumulative effect of both types of costs, in terms of latency and power consumption, giving equal weights to both.

3.4 Summary

IoT networks are generating huge amount of data which raise many challenges in terms of data storage, data processing and data fetching. Cloud computing is proposed to handle this Big Data, but has few shortcomings for some IoT use cases having special requirements. Fog computing is suggested as an companion to cloud platform. In fog computing, processing and applications are concentrated in devices at the network edge rather than transfer to cloud for processing. Therefore, all processing is done at smart devices in the network not in the cloud. In other words, fog will help to move portions of cloud based applications closer to the devices that use them. It is not an easy task to figure out which software tasks to decouple from the cloud, but due to rapid growth of IoT networks and related challenges, we have to take a different approach to cloud computing.

We have studied an interplay of cloud and fog in real time smart parking system as a use case. Use of foglets improve efficiency and latency. We distribute the processing tasks between users and distant servers to improve upon the service time. Thus our proposed system leads to more efficient, safer and environment friendly driving conditions.

References

1. Sarkar, S., Chatterjee, S., & Misra, S. (2015). Assessment of the suitability of fog computing in the context of internet of things . In *IEEE Transaction on Cloud Computing, 34* (pp. 1–14).
2. Jalali, F., & Hinton, K. (2016). Fog computing may help to save energy in cloud computing. *IEEE Journal on Selected Areas in Communications, 1*, 1–12.
3. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *IEEE Journal and Magzines, 44*, 51–58.
4. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *ELSEVIER Future Generation Computer System, 29*, 1645–1660.
5. Mattern, F., & Floerkemeier, C. (2010). From the internet of computers to the internet of things. *ACM Digital Library, 33*, 107–121.
6. Atzoria, L., Ierab, A., & Morabito, G. (2010). The internet of things: A survey. *ELSEVIER Computer Networks, 54*, 2787–2805.
7. Zugenmaier, A., & Walte, T. (2007). Security in pervasive computing calling for new security principles. In *IEEE Conference on Pervasive Computing* (pp. 96–99).
8. Weiser, M. (1999). The computer for the 21st century. *ACM Digital Library, 1*, 94–110.
9. Hayat, Z., Reeve, J., & Boutle, C. (1999). Ubiquitous security for ubiquitous computing. *ACM Digital Library, 15*, 434–441.

10. Bussard, L., & Roudier, Y. (2002). Authentication in pervasive computing. In *Workshop on Security in Ubiquitous Computing* (pp. 1–5).
11. Osmani, V., Balasubramaniam, S., & Botvich, D. (2007). Fog computing may help to save energy in cloud computing. In *IEEE Journal on Selected Areas in Communications (JSAC)* (pp. 254–258).
12. Mayrhofer, R., Gellersen, H., & Hazas, M. (2007). *Security by spatial reference: Using relative positioning to authenticate devices for spontaneous interaction*. Lecture notes in computer science. New York: Springer.
13. Lai, C.-F., Song, D.-Y., Hwang, R.-H., & Lai, Y.-X. (2016). A QoS-aware streaming service over fog computing infrastructures. In *IEEE Digital Media Industry and Forum* (pp. 94–98).
14. Bonomi, F., Milito, R., & Natarajan, P. (2015). Fog computing: A platform for internet of things and analytics. In *A roadmap for smart environments, studies in computational intelligence* (pp. 169–186). New York: Springer.
15. Rhodes, B. (1997). The wearable remembrance agent: A system for augmented memory. In *International Symposium on Wearable Computers* (pp. 123–128).

Chapter 4
IoT Applications and Business Models

Syed Ahsan Raza Naqvi, Syed Ali Hassan, and Fatima Hussain

4.1 Introduction

The Internet of Things (IoT) provides a notion of sensors or "things" being connected anytime, anywhere. It is considered to be an extension of the Internet to the real world consisting of physical objects, and is often associated with such terms as "ubiquitous network," and "cyber physical system" [1]. All future advancements in the field of IoT are contingent on developments in microelectronics, embedded systems and network protocols.

This chapter aims to provide the reader an overview of some of the fields that IoT can potentially revolutionize in the years to come. It discusses how IoT can change the way we will travel along national highways, how everyday garments may 1 day become more than just pieces of fabric, how two-way communication will play a major role in future electric grids and how it is helping to preserve endangered species like rhinos. Along the way, we outline some hurdles faced by IoT developers and how information security will shape future IoT networks. The chapter closes with a summary of business models that vendors may follow as IoT devices become increasingly pervasive in the market.

S.A.R. Naqvi
The University of Alabama, Tuscaloosa, AL, USA

S.A. Hassan
School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_4

4.2 Applications of IoT

As will be seen in subsequent subsections, the applications of IoT are many and varied and the field has witnessed rapid growth in recent times. Therefore, in order to ease the development process of IoT applications, developers should move beyond low-level cloud programming models. In order to address this problem, [2] proposes a framework that is mapped to cloud application program interfaces (APIs) provided by platforms like Aneka. The framework not only reads data from both the sensors and online databases but also passes messages in case an event of interest is observed. The design is summarized in Fig. 4.1.

Generally, IoT is said to consist of the following layers [3]:

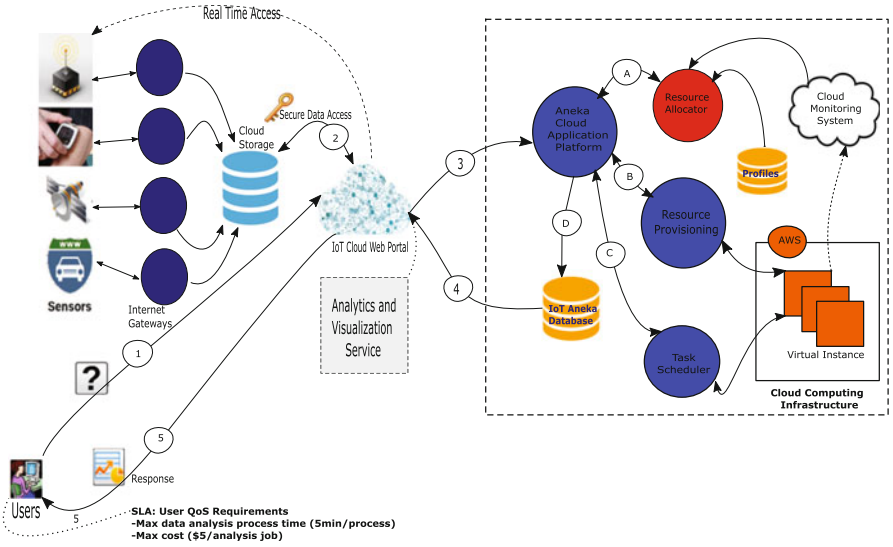

Fig. 4.1 Possible framework for developing future IoT applications

- Physical thing: It is the physical object, such as a light bulb, that provides direct benefits to the consumer.
- Sensor/actuator: The first layer is equipped with a minicomputer complete with sensors and actuators. The sensors are responsible for collecting data about the physical object and/ or its surroundings, whereas the actuator takes an appropriate measure in response to this data. For instance, a sensor might be used to determine whether or not there is human presence in the vicinity of a light bulb. Depending on this information, the actuator can turn the bulb either on or off.

(continued)

- Connectivity: The second layer is globally accessible through the internet to subscribers around the globe.
- Analytic: This layer collects and stores data originating from the sensors and checks for its plausibility.
- Digital service: The final layer packages the digital services offered by the previous layers in a suitable form.

4.2.1 Intelligent Transportation

It is expected that in the near future the principle of IoT could be applied to vehicles so as to set up car networks aimed at exchanging high rate multimedia information for entertainment purposes [4]. Such networks are called Vehicular Ad-Hoc Networks (VANETs). Device-to-device (D2D) communication is one of the promising applications of network control over communication sessions, whereby the devices discover each other and directly communicate with minimal involvement of the network. This strategy can help overcome latency issues in scenarios where vehicles communicate directly with each other, i.e., vehicle-to-vehicle (V2V) communication [5]. The resulting VANET converts the participating vehicle into a wireless router or node, allowing other cars within a proximity of 100–300 m of each other to connect and create a network. Vehicles moving out of this range are dropped from the network.

Vehicular communication is considered to be a front-runner in ensuring the security and the efficiency of future transportation systems by relaying information such as changes in the ambient conditions (snow, fire etc.) and traffic conditions in general (road accident, on-going construction work or congestion) (http://www.nautilus6.org/events/0701-WONEMO/20070115-WONEMO-Automotive.pdf). With each vehicle communicating in its neighborhood with unknown and unspecified vehicles on the road, V2V communication can prove to be vital for collision avoidance techniques as the distance and speed of the nearest neighbor is given greater importance in such situations.

There have already been other major developments towards achieving ‘smartness’ on the road. Multi-national enterprises around the world have made locating parking slots easier through sensors (ParkSight [6]), allowed users to summon cabs through a single tap of a smartphone (Uber [7]) and designed a mechanism for volunteers to collect road condition data for visualization on a map to be used by

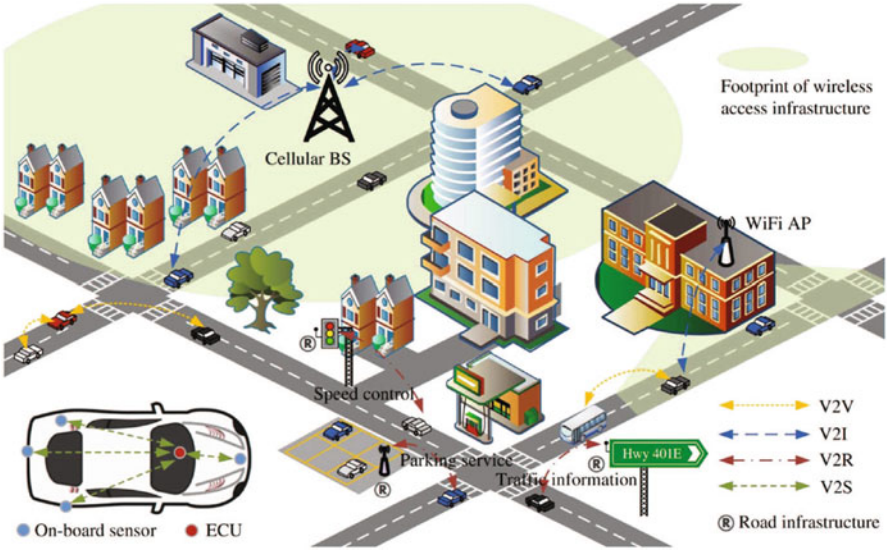

Fig. 4.2 Communication techniques expected to be used in VANETs comprising vehicles equipped with on-board sensors and electronic control unit (ECU); vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-road side unit (V2R) and vehicle to sensors (V2S) (https://ece.uwaterloo.ca/~kan.yang/securitybbcr/vanet.html)

both individual users and the authorities (Streetbump [8]). Needless to say, IoT is expected to continue playing a major role in determining how drivers interact with the environment, including the traffic, around them. Figure 4.2 summarizes the various communication techniques expected to be used in VANETs.

4.2.2 Smart Clothing

The state-of-the-art for smart clothing is restricted to special purpose, low-volume fabrics that are embedded with electronics. Related literature, however, projects the use of IoT in future garments by incorporating sensing layers, such as a conductive coating or a mesh of conductive threads, into a cloth during production. In particular, [9] lays down three requirements for achieving this:

- The sensor layers need to be tailored depending on what variables they aim to sense and the body location they are supposed to perform their job on.
- There should be a connectivity between the sensor layers to furnish a power and communication infrastructure for the sensory components.
- There should be an interface to set up the cloth to be embedded with electronic circuitry.

In conjunction to the aforementioned features, a separate operating system may be added to the electronic control modules.

IoT can also find application in product inspection and quality control. For instance, [10], proposes the design of a garment hanger that not only checks the appearance of the cloth (such as color and fitting) so that it meets predetermined standards, but also determine its tensile strength as well as its response to being worn by a person several times.

Researchers have also looked into the possibility of developing a sensor system to determine the optimal temperature for a building's heating or cooling system depending on the clothing insulation of the occupants [11]. The work was undertaken to prevent wastage of energy as well as reduce the feelings of discomfort experienced by people inside the building owing to inordinately high or low temperature settings. A smart sensor system for clothing insulation inference (SiCILIA) is a platform that addresses these challenges by obtaining the personal and physical variables of the inhabitant's thermal environment to deduce their clothing insulation.

4.2.3 Smart Grids

Earlier, the functionality of smart meters was restricted to measuring the electricity used and the ability to remotely control the supply and cutoff when necessary. However, the prospects of incorporating IoT principles into future electric grids have meant that smart meters will be able to perform a more diverse set of operations in the smart grid. These include, but are not limited to, real-time determination of electricity consumption with the possibility of remote and local reading of the meter, linkage with other utilities such as gas and water supply and recording events such as device status and power quality [12].

> It would be instructive to note that while the smart meter is taken to be the data capture device, it may be connected to a communication device such as a smart meter gateway for setting up a secure network. This gateway could receive and communicate real-time information from the supplier and even start and stop power supply.

In addition, this gateway could also be connected to household appliances and is responsible for relaying consumption information to the subsequent level in the smart grid. In the long term, it has also been suggested that smart meters will also replace the large number of sensors currently being used in the grid by relaying voltage and current measurements directly to an aggregation point, thus reducing cost [13]. In literature, several communication techniques have been considered

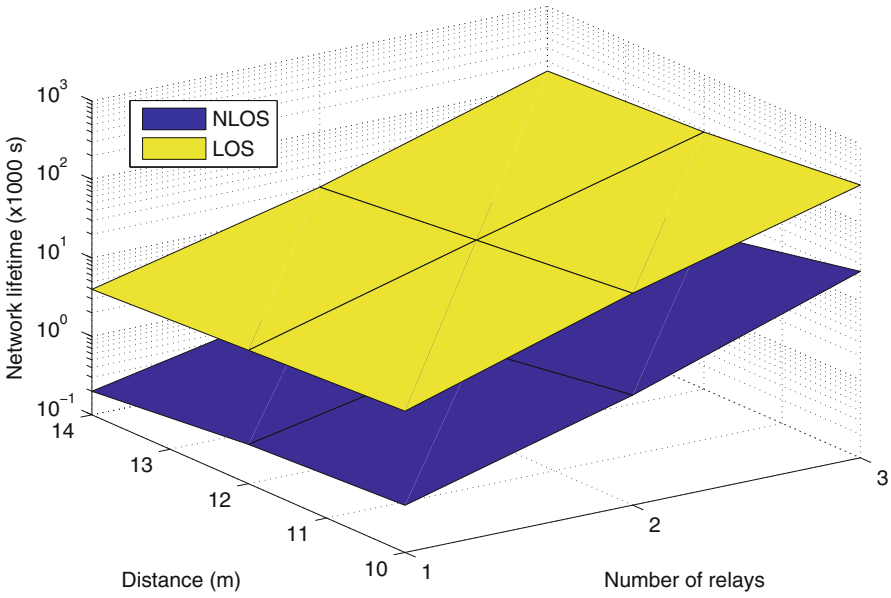

Fig. 4.3 Trade-offs between the number of cooperating relays, coverage distance and network lifetime

for use in transmitting this information in the neighborhood area network (NAN) of a smart grid. For instance, [14] develops a test bed using software defined radios (SDRs) to relay data from a source node, to multiple relays and then on to the destination node using cooperative communication. The setup has been tested in both indoor and outdoor environments. The paper showed that increasing the number of relays not only helped improve the coverage distance to achieve the same quality-of-service (QoS) but also offered better network energy efficiency as compared to systems that do not employ cooperative communication. Figure 4.3 illustrates one of the findings of the paper. The graph provides credence to the claim that increasing the number of relays to achieve the same QoS helps increase the network lifetime. This result is especially important considering the fact that most, if not all, sensors in an IoT network run on battery.

In addition to this work, [15] develops a media access control (MAC) protocol for such a network. Figure 4.4 outlines one set of results obtained by the authors. The figure shows the variation in throughput for increasing source-destination (S-D) distances at different transmit powers for single-input single-output (SISO) and cooperative links. An important observation from the plot is that the throughput performance of a cooperative network with a source transmit power of 5 dBm is comparable to that of a SISO network with a transmit power of 10 dBm.

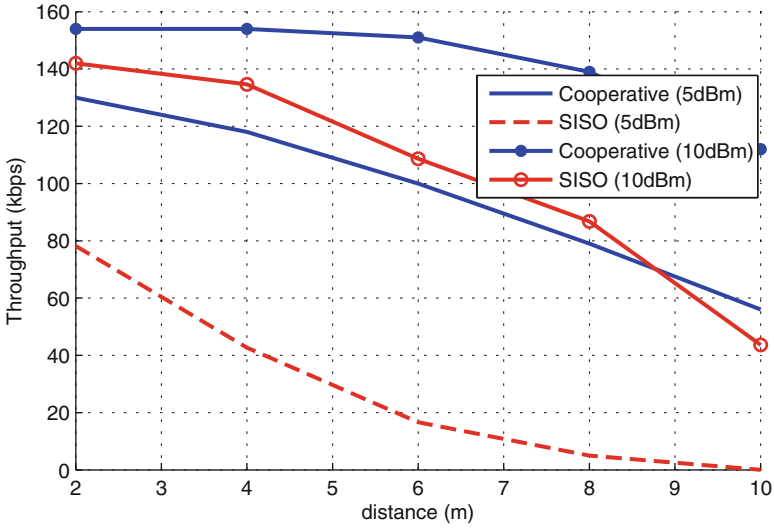

Fig. 4.4 Throughput versus S-D distance for SISO transmissions and CT

4.2.4 Education

With the vast proliferation of internet access, students and researchers now feel the urge to not only access the work of experts in their field but also their peers. The Internet has thus become a platform for sharing ideas and on-going research. It is expected that in the future experts in a particular area will be requested to teach classes anywhere in the world through streaming or live video [16].

Global education received a major boost with the introduction of massive open online courses (MOOCs). With the world's leading universities providing access to their professors free of charge, the idea of "flipped classrooms" is gaining strength, whereby students would be expected to learn the subject matter *outside* the classroom, leaving the course instructor to discuss problems and ideas during class time. By providing an opportunity for students in the developing world to learn beyond basic education (which is often limited by the economic status), MOOCs and other online resources like the Khan Academy [17] can, in time, help improve the quality of life for people who cannot afford higher education. Another major group of beneficiaries would be home-bound individuals who are capable of learning and participate in classroom courses.

In the future, MOOCs may transform into vehicles for two-way information which can prove vital for the universities and teachers engaged in furthering these initiatives. MOOCs can generate data-sets outlining the number of registrations and drop-outs, online attendance per course and the students' internet protocol (IP) address of the students. The universities can thus gauge the time that people spend on course materials and narrow down the content and topics that might be popular

among specific demographics. This would allow course instructors to streamline their teaching methods to reduce drop-out rates and to align the curriculum to the students' needs.

4.2.5 Environment Observation, Forecasting and Protection

With the environment under constant stress due to extensive urbanization and adverse human activities such as hunting for sport, IoT is projected to play a part in preserving natural resources and endangered species. In order to achieve the latter objective, organizations around the world are using GPS-enabled devices to track the habits and health of endangered species (http://industrialiot5g.com/20161118/channels/fundamentals/iot-impact-environment-tag31-tag99). In fact, Cisco is using long range radio (LoRa)-based connectivity to track the movement of anyone entering the reserve grounds for rhinos (http://www.cisco.com/c/m/enus/never-better/csr-1.html). In case of trespassing, precautionary measures may be taken for the well-being of the animals.

Furthermore, IoT can potentially help alleviate waste management issues particularly in countries like the USA where the daily per capita trash was estimated to be 4.6 pounds in 2013 [18]. By determining the optimum time for waste collection and the best routes for the trucks to follow, IoT can redress the problems associated with waste build-up in neighborhoods.

With an increasing number of water-stressed countries around the world, the installation of smart water sensors in buildings can also help limit domestic water consumption. Through these devices and data analytics, users will be able to keep track of how much water was used in a given period, allowing them to cut down on excessive usage.

Another major environmental crisis that the world faces is deforestation. In addition to fighting forest fires, drones are now part of an initiative by BioCarbon Engineering to replant one billion trees [19]. The organization aims to achieve its goals through precision agriculture techniques, the use of technology to reduce manpower requirements and cost and the deployment of drones to determine the landscape of the area affected by deforestation.

Finally, IoT can also assist in predicting and mitigating the effects of natural disasters. In particular, Zizmo [20] uses cloud connected sensors that detect motion near earthquake epicenters to issue a warning to residents in the surrounding areas. Similarly, Avatech [21] uses pressure sensors to predict the likelihood of an avalanche.

4.2.6 *Smart Agriculture and Farming*

As stated earlier, the world's water reservoirs are fast depleting and there is an urgent need to conserve this precious resource. According to an estimate, farmers use 70% of earth's freshwater, 60% of which is lost due to faulty irrigation systems, inefficient agricultural techniques and the cultivation of thirsty crops (http://industrialiot5g.com/20161118/channels/fundamentals/iot-impact-environment-tag31-tag99). Sensors and actuators can provide growers with a better visibility over their operation and thus allow them to minimize water wastage by monitoring metrics such as temperature and water pressure. In this respect, Microstrain [22] has developed a system of wireless sensors to gauge key conditions during the growing season in vineyards. The sensors measure variables such as temperature, soil moisture and solar radiation and alert the farmers in case of extreme conditions. Figure 4.5 spells out the possible applications of IoT in farming.

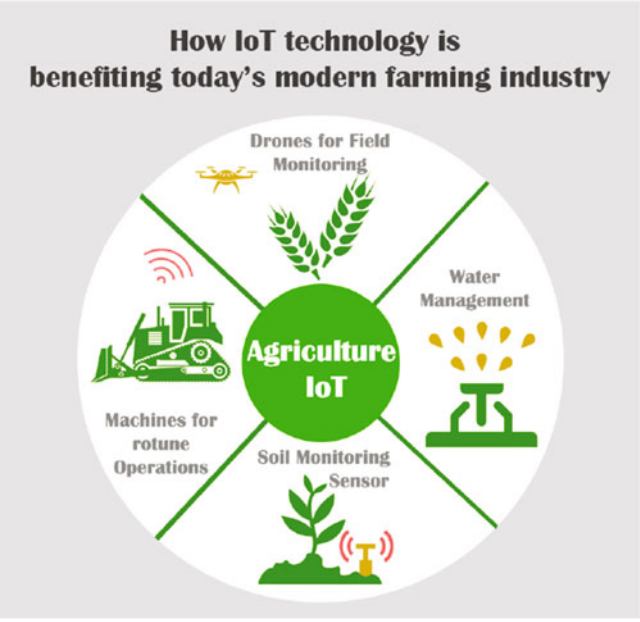

Fig. 4.5 Applications of IoT in agriculture (https://blog.beaconstac.com/2016/03/iot-ecosystem-iot-business-opportunities-and-forecasts-for-the-iot-market/)

4.2.7 Health Care

Given the vast number of future applications of IoT, it is little wonder that IoT is expected to revolutionize health care as well. In particular, IoT can allow physicians to constantly monitor the physiological parameters of their patients. Owing to the recent advances in wireless sensor networks (WSNs) and embedded systems, miniaturized health monitoring devices have become a reality. These sensors can form a body sensor network (BSN) which not only monitors the patients' health indicators but also incorporates context aware sensing for improved sensitivity. In this connection, [23] proposes the design of a hardware development platform.

The diagnosis of cardiac diseases by constantly monitoring the patient's electrocardiogram (ECG) signals is a common application of BSNs. These sensor networks have also been used for monitoring patients with Parkinson's disease as they offer credible data collected over a larger period of time, compared to the inferences made through clinical observation. For example, in [24], the authors used wearable sensors to identify the movement characteristics of patients suffering from Parkinson's disease and attained real-time monitoring with high accuracy. Similarly BSNs have also been used for the treatment of respiratory diseases. In such a scenario, the network comprises a respiratory sensor for determining the depth and frequency of breathing. The collected data might then be used for patients to undergo breathing training which is instrumental in respiratory disease rehabilitation. The setup includes It utilizes a respiratory sensor for monitoring depth and frequency of breathing, so as to guide patients to take correct breathing training, which plays a very important role in respiratory disease rehabilitation [25, 26]. Figure 4.6 summarizes the different components of a BSN.

4.2.8 Smart Homes/Buildings and Monitoring

Sensors can prove useful in preventing possible health hazards at home. For instance, environmental sensors can now monitor air quality, barometric pressure, carbon monoxide concentration, color, gas leaks, humidity, hydrogen sulfide levels and temperature, with upcoming start-ups offering users to access these details remotely. Netatmo [27] is one such venture. Other enterprises have tried to incorporate IoT principles to household lighting. Meethue [28], for example, is a bulb that can be controlled by mobile devices that is sensitive not only to the weather but also to user preferences, time and room activity. Additionally, some smart home solutions have also focused on facilitating the activities of the elderly. For instance, Ubi [29] a voice-activated computer allows access to an audio calendar, podcast and voice memos, and can also make lighting-based notifications to indicate the occurrence of certain events [30].

IoT principles have also been put to use to ensure building safety. Certain start-ups have developed sensors that can be embedded into the foundations allowing

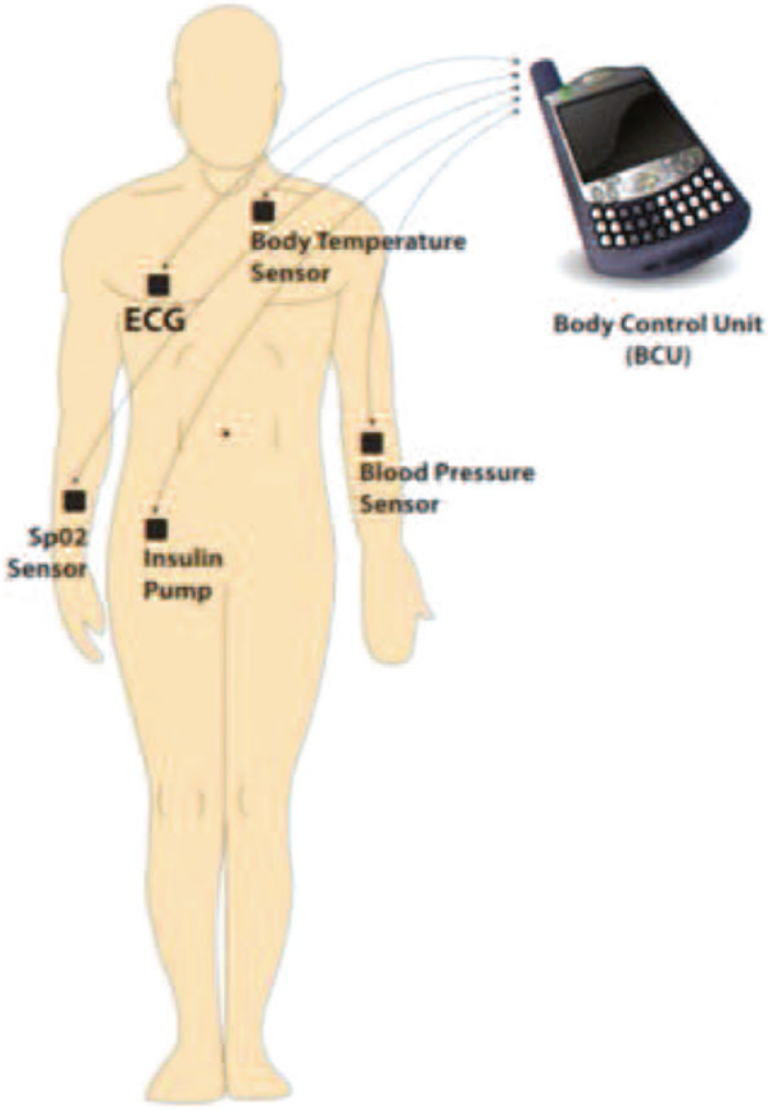

Fig. 4.6 Components of BSN (https://www.elprocus.com/ban-body-area-network/)

for consistent load monitoring, as well as those that can be used to maintain lifts and heating systems. Moreover, certain remote fire extinguisher monitoring systems have been developed which alert the user in the event of the fire extinguisher being absent from its designated position or its pressure falling below safe operating levels.

4.2.9 Public Safety

One manner in which IoT can facilitate public safety is through D2D communication [31]. Massive deployment of devices could help in multi-hop communication between the source and destination. Most of these devices utilize battery power so the network devised for disaster scenarios must be energy efficient. In post disaster scenario several of the devices are damaged and hence are unable to support the communication. The owners of the hand held devices can block any outside control thereby hindering the transmission. Viewing the sensitivity of the information in disaster and terrorism scenarios, the blockage of transmission is not affordable. The network needs to be resilient and be able to self-organize in case of any such situation. Similarly, several nodes might not be available for transmission due to low battery power. If the nodes reconfigure transmission protocols automatically there is a fair chance that the information is delivered to the destination. In case of disaster scenarios a "disaster mode" could be activated which is based on special routing for low power transmission and avoids any unwanted communication between devices. IoT has also been projected to play a major role in crowd management [32].

4.3 Research Challenges

Although IoT has opened up many exciting avenues for future development, researchers continue to grapple with roadblocks obstructing its expansion. This section will aim to delineate some of these challenges.

4.3.1 Versatile Sensors and Technologies

The first challenge deals with the sheer number of disparate sensor nodes, which cause a sensor network employing IoT to become a very complex heterogeneous network. With a wide array of networks employing several different communication techniques, IoT-based systems lack a common platform to provide a transparent naming service [33]. In addition, given the volume of data being transmitted the system frequently encounters latency and other communication issues [34]. The development of network protocols to ensure the smooth movement of data obtained from many different sensing devices within an IoT-enabled system is a major research challenge in itself. Modularity is also a key feature of IoT networks [30]. It refers to the concept of consumers building a smart object of their own without being restricted to products from a single vendor.

4.3.2 Integration of IoT and Conventional IT

There is also a need to combine IoT with conventional information technology (IT) systems to form a unified information structure. Integrating IoT devices with extant software systems would also demand the development of middleware. Furthermore, the large number of sensors that make up an IoT network produce large amounts of real-time data that may not be readily useful to the end consumer. The end-users would have to possess strong big data skills to make sense of the available information, which could be very challenging in itself.

4.3.3 Standardization

Another problem that needs to be looked into is standardization, which is aimed at improving interoperability of different application which in turn enhances performance. The new IoT standards should allow different types of sensors manufactured in various countries to exchange information [35]. In addition they should not only address radio access level and security issues [36–38], but also offer modifications that fit the needs of particular industries as well.

4.3.4 Security Protocols

One of the most crucial aspects of standardization in IoT is the development of security protocols to ensure privacy protection. The dependence of IoT networks on the cloud server makes such systems susceptible to cyber attacks. The current provisions for information security in IoT networks do not necessarily meet the strict requirements of certain industrial applications. Developing an encryption technology for IoT networks is expected to be more challenging than in the case of WSNs as the former allows several daily "things" to be connected and monitored, collecting a large volume of private data over a considerable period. One situation in which information security is essential is the case of self-driving cars of the future. These cars would be able to use VANETs to exchange, for example, data about distance and speed to avoid collisions. However, a malignant cyber attack on such vehicles could cause false data to be generated, putting lives at risk. Another scenario could include a BSN communicating a patient's physiological parameters to a physician. In the absence of reliable security protocols, there is a possibility of the patient's data being compromised, breaching doctor-patient confidentiality.

4.4 Business Models

A business model is defined as the plan implemented by a company to generate revenue and make a profit from operations (http://www.investopedia.com/terms/b/businessmodel.asp).

> Given the nature of the IoT ecosystem, organizations not only have to collaborate with the firms from other industries but also their own competitors [39], which means that conventional business models are not applicable to the IoT phenomenon.

The authors in [40] stated that the current challenges of IoT include the vast number of connected objects in such networks, the fact that recent IoT innovations are yet to be tailored into products and services and a lack of clarity regarding the structure, governance and stakeholder roles in this emerging field.

Different frameworks of IoT related business models have been investigated in literature. For instance, [41] presented a 'D(esign) N(eeds) A(spirations)' model for IoT businesses, with 'design' referring to the key components of the system (including resources and activities), the 'needs' being customer relationship and 'aspirations' being the end result desired by the business e.g. revenue.

> One of the unique features of IoT services is that customer behavior and feedback can be monitored consistently allowing businesses to incorporate newer features into the product. Thus, IoT bears the concept of service-dominant business model.

The model could also be used for effective forecasting and process optimization [42]. In this service-dominant business model [43], customers and firm are considered to be partners in the value creation process, in contrast to conventional models that project the latter as the sole value creators. The service-dominant model is an example of a network-centric view in IoT business which has been elaborated upon by [44] by proposing a service-based business model. The key elements of this model, along with associated issues, are summarized in Table 4.1.

Furthermore, authors in [3] also formulates a business model specific to IoT, consisting of six components listed in Table 4.2, terming the model as *Digitally charged products*. The paper describes physical freemium as some physical asset which is sold along with a free digital service, say digital installation and maintenance instructions, at no additional cost. Digital add-on refers to customers acquiring added services on top of what is offered by the product. These "add-ons" may be provided by the original vendor or by any third party enterprise. Digital lock-in

Table 4.1 Service based business model parameters [44]

Value proposition	Articulated offering
	Visualization
	Closer customer interaction
	A dynamic offering portfolio
Revenue mechanisms	New revenue model
Value chain	Dedicated roles for service development
	A structured service development process
	A new reward system
	Extending the resource base
Value network	Finding partners that can add value to the new offerings
	Competitive strategy
	Branding
	Differentiation
	Target market
	New customer segmentation

Table 4.2 Components and business model pattern in IoT [3]

Business model pattern	Components
Digitally charged products	Physical freemium
	Digital add-on
	Digital lock-in
	Product as point of sales
	Object self service
	Remote usage and condition monitoring

refers to a sensor-based, digital handshake which not only prevents counterfeits but also helps ensure warranties. The consumer pointing their smartphone at a product and accessing a web-site selling the same product, including accessories, is an example of products becoming points of sale. Object self-service refers to "things" serving themselves, such as a heating system ordering an oil refill when needed. Finally remote usage and condition monitoring refers to the constant connectivity of sensors to the internet where they upload real-time data which can be used to take corrective action in the case of an unusual event.

4.5 Conclusion

In this chapter, we aimed to summarize how IoT devices are changing the way we live and interact with the physical world. As IoT networks become increasingly complex and widespread, businesses around the world would have to rethink the process of value creation. Despite lingering concerns such as information security, it is safe to state that IoT can potentially bring about economic development which could be at par with that witnessed during the Industrial Revolution.

References

1. Zheng, L., et al., (2011). Technologies, applications, and governance in the internet of things. In *Internet of things-Global technological and societal trends: From smart environments and spaces to green ICT*. River Publisher series in Communication.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
3. Fleisch, E., Weinberger, M., & Wortmann, F. (2014). Business models and the internet of things. In *Bosch IoT Lab White Paper*.
4. Boeglen, H., Hilt, B., Lorenz, P., Ledy, J., & Poussard, A. (2011). A survey of V2V channel modeling for VANET simulations. In *8th International Conference on Wireless On-Demand Network Systems and Services, Bardonecchia* (pp. 117–123).
5. Nshimiyimana, A., Agrawal, D., & Arif, W. (2016). Comprehensive survey of V2V communication for 4G mobile and wireless technology. In *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), India* (pp. 1722–1726).
6. ParkSight: The complete smart parking solution, Streetline, Inc., Foster City, CA, USA, Tech. Rep., 2016.
7. Uber. (2016). *Uber* [Online]. Available: https://www.uber.com/
8. All Traffic Solutions. (2016). *All Traffic* [Online]. Available: http:/www.alltrafficsolutions.com/smartapps-video/smartapps-overview/
9. Cheng, J., et al., (2013). Smart textiles: From niche to mainstream. *IEEE Pervasive Computing, 12*(3), 81–84.
10. Wong, Y., & Ip, K. (2010). A three in one smart garment hanger. In *International Conference on System Science and Engineering, Taipei* (pp. 50–55).
11. Shaabana, A., Zheng, R., & Xu, Z. (2015). SiCILIA: A smart sensor system for clothing insulation inference. *IEEE Global Communications Conference (GLOBECOM), USA* (pp. 1–6).
12. Gerwen, R., Jaarsma, S., & Wilhite, R. (2006). *Smart Metering. Leonardo Energy (White Paper)* [Online]. Available: http://www.leonardo-energy.org/sites/leonardo-energy/files/root/pdf/2006/SmartMetering.pdf
13. Ilic, D., Karnouskos, S., & Da Silva, P. (2012). Sensing in power distribution networks via large numbers of smart meters. In *Proceedings of the 3rd IEEE PES International Conference and Exhibition on Innovative SmartGrid Technologies (ISGT'112)* (pp. 1–6).
14. Omar, M. S., et al., (2016). An experimental evaluation of a cooperative communication-based smart metering data acquisition system. *IEEE Transactions on Industrial Informatics, PP*(99), 1–1.
15. Amin, S., et al., (2016). Implementation and evaluation of a cooperative MAC protocol for smart data acquisition. In *IEEE 83rd Vehicular Technology Conference (VTC Spring), China*.
16. Selinger, M., Sepulveda, A., Buchan, J. (2013). Education and the internet of everything: How ubiquitous connectedness can help transform pedagogy. *Education IoE Whitepaper, Cisco*.
17. Khan Academy. *Khan Academy* (2016). [Online]. Available https://www.khanacademy.org
18. Report on the Environment (2013). *United States Environmental Protection Agency* [Online]. http://www.epa.gov/roe/
19. BioCarbon Engineering: Industrial scale reforestation services (2016). [Online]. http://www.biocarbonengineering.com/
20. Zizmos: Earthquake early warning system (2016). [Online]. https://www.zizmos.com
21. Avatech (2016). [Online]. http://avatech.com/
22. MicroStrain, Inc. (2016). *Shelburne Vineyard Remote Monitoring*. [Online]. Available: http://www.microstrain.com/news/shelburne-vineyard-relies-wireless-sensors-and-cloud-monitor-itsvines
23. Lo, B., Thiemjarus, S., King, R., & Yang, G. (2005) Body sensor network - A wireless sensor platform for pervasive healthcare monitoring. *Proceedings of 3rd International Conference Pervasive Computing* (pp. 77–80).

24. Patel, S., et al., (2006). Analysis of the severity of dyskinesia in patients with Parkinson's disease via wearable sensors. *Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks, USA* (pp. 4–126).
25. Mitchell, E., et al., (2010). Breathing feedback system with wearable textile sensors. In *Proceedings of the 2010 International Conference on Body Sensor Network (BSN), Singapore* (pp. 56–61).
26. Bates, A., et al., (2010). Respiratory rate and flow waveform estimation from tri-axial accelerometer data. *Proceedings of the 2010 International Conference on Body Sensor Network (BSN), Singapore* (pp. 144–150).
27. NetAtmo: Urban weather station (2014). Household Technol. PTY Ltd., Durban, South Africa.
28. *Meet Hue Personal Wireless Lighting*, Koninklijke Philips, Amsterdam, the Netherlands. http://www2.meethue.com/en-us/
29. Unified Computer Intelligence Corp. (2016). *UBI* [Online]. Available: http://theubi.myshopify.com/.
30. Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. In *IEEE Transactions on Emerging Topics in Computing, 3*(4), 585–598.
31. Huang, G., et al., (2016). D2D relaying based multicast service in Public Safety Networks. In *35th Chinese Control Conference (CCC), China* (pp. 6923–6927).
32. Kantarci, B., & Mouftah, H. (2014). Trustworthy sensing for public safety in cloud-centric internet of things. In *IEEE Internet of Things Journal, 1*(4), 360–368.
33. Miorandi, D., et al., Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516 (2012)
34. Xu, L. D., He, W., & Li, S., (2014). Internet of things in industries: A Survey. In *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
35. Miorandi, D., et al., (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.
36. Wang, F., et al., (2013). A system framework of security management in enterprise systems. *Systems Research and Behavioral Science, 30*(3), 287–299.
37. Li, J., et al., (2013). A top-down approach for approximate data anonymisation. *Enterprise Information Systems, 7*(3), 272–302.
38. Xing, Y., et al., (2013). Operations research (OR) in service industries: A comprehensive review. *Systems Research and Behavioral Science, 30*(3), 300–353.
39. Chan, H. (2015). Internet of things business models. *Journal of Service Science and Management, 8*, 552–568.
40. Westerlund, M., Leminen, S., & Rajahonka, M. (2014). Designing business models for the internet of things. *Technology Innovation Management Review, 4*, 5–14.
41. Sun, Y., Yan, H., Lu, C., Bie, R., & Thomas, P. (2012). A holistic approach to visualizing business models for the internet of things. *Communications in Mobile Computing, 1*, 1–7.
42. Hui, G. (2014). How the internet of things changes business models. *Harvard Business Review, 8*, 552–568.
43. Turber, S., et al., (2014). Designing business models in the era of internet of things. In *9th International Conference DESRIST, USA* (pp. 17–31).
44. Kindstrom, D. (2010). Towards a service-based business model-key aspects for future competitive advantage. *European Management Journal, 28*, 479–490.

Chapter 5
Summary and Conclusions

Fatima Hussain

5.1 Smart World and Internet of Things

Vision of smart world is the topic of research from many years and various collaborative and individual research and technical communities are working on it. Meaning of "smart" is anything that has a capability of autonomously acquiring and processing information, and has capability of applying this gathered knowledge having adaptability capabilities according to its inhabitants. Combining the physical and virtual world convergence, IoT has a potential to make this dream come true. IoT will have personalized and predictive impact on the way human live and work, thus making their lives easier and safer.

Targeted ventures for this smart world such as smart city, smart phone, smart home, smart building, and smart health are few to name. Prominent research communities working on this agenda are generally; internet of things (IoT), wireless sensor networks (WSN), pervasive computing (PC) and cyber physical systems (CPS). It is further supported by applying knowledge of artificial intelligence, machine learning based decision making, signal processing, real time computing and human computer interaction vision. In addition to this, immense development in the field of integrated electronics and computer technology has supported the inclusion of sensors and actuators in our daily life, to make it smarter.

IoT is the most widespread innovative technical paradigm and is envisioned to connect and involve all the things/humans across the globe. The scope of IoT is

F. Hussain (✉)
Assistant Professor, School of Computer Science, University of Guelph, Guelph, ON, Canada

Research Associate, Department of Computer Science, Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON, Canada
e-mail: fhussa03@uoguelph.ca; fatima.hussain@ryerson.ca

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1_5

enormous and will affect every aspect of all our lives, in future. As IoT is interconnected gathering of smart devices, machines and humans; it should be equipped with heterogenous operating systems and communication technologies of varying properties and protocols. Throughout in this book, various blocks mandatory, to build complete architecture of IoT, are discussed in very straight forward and simple way.

In this chapter, I will briefly summarize the IoT domain and its contributing blocks. Recent advancements and research flourished in it's various domains is also discussed. At the end few research challenges and suggested methods leading to potential solutions are listed.

5.2 Key Concepts

5.2.1 Sensing and Information Gathering

IoT is mostly comprised of sensor nodes and relays to provide distributed and intelligent sensing services. WSN is considered to be the most important building block of IoT. With technical advancement in integrated circuits, sensing and actuation utility are extended to home, environment, devices and even to human bodies. This information sensed and gathered by humans/machines is used for actuating various tasks in health, security and entertainment areas. These sensor nodes are interconnected through various communication technologies and protocols.

5.2.2 Information Communication

Information gathered from smart things and devices has to be communicated and exchanged through suitable connecting technologies. It is very difficult to design single communicating protocols applicable unanimously for all smart devices. Characteristics of required communication protocol are based on requirement of data rate, power and communication range of smart devices. These characteristics are specific to respective applications and information actuation. For instance, e-health monitoring bands require low power and short distance RFID or ZigBee technology compared to remote surgery and operations, demanding high data rate WiFi or WiMAX communication.

5.2.3 Information Processing and Management

Data from smart devices is collected for plausibility, and is classified and integrated/processed with other services for desired actuation. Data generated by all the smart devices is enormous in amounts and require efficient data processing, mining and

management techniques. Due to these huge amounts of generated data, local storage and processing becomes difficult. Cloud computing is the platform which provides low cost resources for data monitoring, management and processing. It provides the on-demand resource access and reduced cost of resource management. Integration of cloud with IoT is a very challenging task, as IoT devices are larger in number, dynamic in nature and have variable quality of service requirements.

5.2.4 IoT Applications

There has been an exponential growth in numerous IoT applications' area due to communication possible among smart devices and things. These things can be car, fridge, clothes etc. having sensing and actuating capabilities. Thus, it leads to development of many IoT application domains resulting into smart environment, smart people with smart living economy, and smart mobility.

Services provided by each application are supported by service requirements for a specific problem. For instance, smart traffic lights and vehicle-to-vehicle communication (V2V) are used to relay and communicate real time data among systems, for implementation of smart transforation system. In smart home environment, security, comfort and power management are achieved through innovative home applications. Smart building, smart city, smart health etc. are few to name and many more applications possible depending upon humans vision and needs. In addition to personal applications, industrial IoT applications are also flourishing at a greater rate. Industrial IoT enables the use of smart devices (things) in manufacturing plants for process control, automation and remote monitoring.

5.2.5 Business Models

In recent years, there is a great progress in technological innovations, due to advancement in intelligent computation and communication technologies. However, development of industrial innovations, related business modes and models are lagging far behind. There is a need or merging and coupling process between technological innovations and business/industrial innovations. Therefore, emerging information technology (IT) has greatly impacted the growth of innovative business models.

Advancements in various domains of IoT enable the innovation of new hybrid business models, comprise of digital and physical systems. E-commerce, crowd-sourcing and crowd-funding are few to mention leading towards new IoT model of digitally charged sensors. We require new business models to enhance and optimize the customer user experience by developing new products. These models should support customer responsiveness and result in dynamic and situation specific pricing/earning models.

Typical dependencies of IoT business model are based upon questions like who, where, why and how. Collaborating partners are "who" and resulting benefits from this partnership answers "why". While position of values creation in layer model of these objects describes "where". IoT tactics and strategies are integrated with entire framework and result into value added network, satisfying the question of "how" [1].

5.3 Recent Research

IoT is the combination of smart heterogenous devices capable of sensing, and communicating with each other, bringing benefits to society and environment. Resulting networks formed with these devices, posses diverse characteristics in terms of capabilities and architecture. As a result, new problems arise in terms of addressing, communication, management, energy and security. There is a need of development in the design of smart devices, communication technologies, intelligent computing and processing algorithms. Current research in few main areas of IoT has been covered throughout the book, and below the prominent points can be found.

5.3.1 Smart Devices and Processors

IoT is comprised of intelligent devices, which are interconnected and can inter-communicate, for making our life smarter. IoT devices have varying capabilities and are mostly comprised of accelerometer in someapplications. Accelerometers are specialized sensors with mechanical and electrical specifications. Traditional embedded systems has evolved into micro-electrical mechanical system (MEMS), with the advancement in multiple technologies and control systems.

There has been a tremendous growth in MEMS from past decade, and it has proven itself to be a promising candidate for numerous innovative IoT applications. Ultra low power consumption, software embedded on hardware, energy harvesting capabilities, simpler interfaces to human body and surfaces, and easier network connectivity makes it an excellent choice for sensing in IoT networks. It has an excellent working potential in applications such as robotics, e-health and wearable devices, automated cars, social and infrastructure monitoring.

5.3.2 Connectivity and Transmission

Typical communication technologies used for inter-operability of IoT devices are WiFi, ZigBee, bluetooth low energy (BLE), RFID and millimeter wave technology etc. [2]. The type and design of each node can be different than other and is specific

to application. It becomes impossible to design such nodes which can work equally well for all types of communication technologies. In addition to this, choice of communication technology depends upon the transmission range and require data rate. Inter-operability and inter-communicability of these heterogenous nodes are a challenge. Differences between various communication technologies and protocols, in terms of packet structure and size, operating frequency and bandwidth need to be considered while designing these networks. For example, a smart phone can communicate with ZigBee sensor via an interface capable of translating protocols being used at the both ends. Therefore, there is a need of designing a common communication protocols to achieve diversity gains and reduce device complexity.

Another approach is to design energy efficient and less complex universal transceivers. A multi-protocol transceiver is proposed to be used in such heterogenous IoT environment [3]. This transceiver can prove to be an common platform to exchange data from various nodes using different technologies such as RFID, ZigBee, WiFi etc. This can allow multi-channel communication among different smart devices with different communication protocols.

Cooperative routing and communication is one of the proposed techniques to cater for heterogenous IoT devices and technologies. There is a need of systematic cooperative techniques for relaying and routing information among IoT devices [4]. Information is carried to the furthest destination by cooperation among various intermediate devices. As massive number of these smart devices are envisioned to be present per unit area, opportunistic relaying is employed to select the best node/device at the time of information transfer. This will also increase the spatial diversity, reduce interference and power consumption and combating against channel fading [5].

In addition to the heterogeneity of IoT devices and applications, communication among massive number of these devices is also a challenge. Sufficient address space for all these devices and energy efficient channel access techniques are problems of utmost importance. IPv6 is considered to be an excellent solution to provide enough address space [6, 7] which is globally reachable for massive IoT devices. It has an ability to multiplex massive channel access of these devices, from heterogenous and diverse IoT applications. IPv6 is the only choice by Internet Engineering Task Force (IETF), for the wireless communication of WSN. As it is the de facto standard for internet and has numerous already developed compatible protocols and processes.

5.3.3 Fog and Transparent Computing

High amount of heterogenous raw data generated by IoT devices raises new challenges in terms of processing and management. Classical methods of data management seem inappropriate considering heterogeneity and uniqueness of IoT applications. Most of the data is user generated from their social networks and is available at the edges, while storage and processing is done in the cloud. Therefore, it calls for the efficient air interface and cloud access network architecture. Despite

the fact that there is a marked research in cloud radio access networks, still requirements of all the heterogenous IoT applications are not met, as it is difficult to process and analyze heterogenous data from varying sources.

Transparent computing is another computing platform that can serve the needs of IoT applications. It is a kind of service computing that separates the software and hardware tasks of cloud computing, such that data storage and computing are processed separately [8].

IoT device has limited bandwidth capabilities and also has constraint resources in terms of battery life. Therefore, cloud is not able to provide services to these devices in timely manner without latency. Fog is a new computing paradigm proposed to manage large number of IoT devices in a distributed way. Fog performs computing and processing at the user end, in contrast to cloud, thus making mini-clouds at the edges. It will help reduce the routing and processing burden from cloud and also improve scalability [9]. Edge entities can share and exchange data among each other without relaying it to cloud, thus reducing end to end latency.

5.4 Research Direction

In the following, research paths/solutions for prominent research challenges are proposed.

5.4.1 Network Management

IoT networks are complex heterogenous networks, and network management and design for potential problems is one of the challenging tasks. To be able to identify potential problems within a network, we should be able to detect events within the network. Event is defined as unusual happenings in a network, such as, increased traffic, link failure, network compromise etc. These events can be collected through both passive and active event detection methods. By making use of machine learning algorithms, any potential problem/ malfunction can be detected, and in fact is inferred from occurrence of unusual events. This detection of events can be helpful not only in removing the causes of event occurrence but also in network healing. We can investigate it from two different perspectives:

- Network Infrastructure Monitoring and Surveillance
- Intruder Detection and Attacks

We can incorporate various supervised and unsupervised machine learning algorithms for different types of network issues, and classify them per various parameters such as network size, network type, intruder types etc. Latency and throughput are two major performance metrics for any network, machine learning algorithms used for anomaly detection and network monitoring should be such that they will not compromise these performance expectations.

5.4.2 Heterogenous Traffic Scheduling in IoT Networks

IoT applications are versatile and may comprise of variable traffic such as: bursty, continuous, and periodic in nature. For instance, heterogenous traffic in smart home environment can be of varying types. It can be a real time traffic such as data being uploaded by surveillance cameras for home security, or non-real time data such as smart lighting or air conditioner's periodic update packets of energy consumed. Former has large data frames with tight bounds on bandwidth and delay while latter is comprised of small packet size with flexibility of bandwidth and latency.

One can design QoS supported scheduling of simultaneous flow of various types of traffic. The scheduling can be improve bandwidth utilization, support desired data rate and can maximize network throughput. One can achieve this in three ways:

- Efficient MAC design, which is flexible enough to support varying data rates and traffic. Z-MAC is considered to be an efficient and flexible hybrid protocol for WSN channel access. We can utilize its hybrid nature for supporting various types and size of traffic in IoT networks. It's contention access layer can support heterogenous traffic while distributed scheduled layer can support priority based traffic, in heterogenous IoT networks.
- We can utilize OFCDM combined with machine learning algorithms to support variable types and amount of traffic, simultaneously. Various network nodes can choose between time/ frequency domain spreadings per amount and type of traffic in a network.
- We can use queuing theory to schedule variable length packets from various applications. We can implement this scheduling in two tiers: First tier may identify traffic from various types of applications and second can schedule according to the size of the data packet.

5.4.3 Resource Coordination Among Foglets

Foglets are considered as enhanced middle-ware processing units capable of offloading delay constrained tasks from the cloud. Distributed and optimized framework is required for flexible and efficient implementation of processing at the edge and in the cloud. Reliable data delivery from/to edges, delivered to/from network/ cloud is important.

If there is lack of resource coordination among these foglets, performance degradation may happen and benefit of using edges is lost. Lack of coordination can be a big problem in many scenarios; for instance, if a group of edges want to deliver correlated data to network/cloud, they may wish to transfer common data units once and by only one edge. Similarly, it holds vice versa and network/cloud want to forward correlated/similar information to only one edge out of group of similar edges. This is only possible if there is coordination among all the edges, still enabling them to work distributively.

- We can achieve this in many ways, but game theory seems more promising in this scenario. We can use game theory to model various foglets/ edges, for achieving conflicting and somewhat mutual goals. We can use cooperative game approach for the collaboration of all of these foglets/edges. They make their autonomous yet collaborative decisions for resource sharing and information transfer.

In addition to this, inherent mobility of these foglets raises the problem of volatility in terms of resources and infrastructure. This volatility can cause problems for autonomous collaboration, but can be eliminated by game theory approach.

References

1. Chan, H. (2015). Internet of things business models. *Journal of Service Science and Management, 8*, 1–17.
2. Ahmed, E., Yaqoob, I., & Gani, A. (2016). Internet-of-thIngs-based smart envIronments: State of the art, taxonomy, and open research challenges. In *IEEE Wirelss Communication* (pp. 1–7).
3. Gunasagarana, R., Kamarudina, L., & Zakariaa, A. (2015). Internet of things: Sensor to sensor communication. In *IEEE Conference on Sensors* (pp. 1–4).
4. Bai, J., Sun, Y., & Phillips, C. (2016). CRRP: A cooperative relay routing protocol for IoT networks. In *IEEE PIMRC* (pp. 1–6).
5. Han, C., & Sun, L. (2016). Toward secure internet of things via hybrid forwarding and opportunistic relaying. In *IEEE ICCC Workshops* (pp. 1–6).
6. Li, Y., & Chai, K. (2016). Distributed access control framework For iPv6-based hierarchical internet of things. In *IEEE Journal on Wireless Communication* (pp. 17–23).
7. Xu, K., Qu, Y., & Yang, K. (2016). A tutorial on the internet of things: From a heterogeneous network integration perspective. In *IEEE Journal on Network* (pp. 1–7).
8. Yaoxue, Z., & Ju, R. (2017). A survey on emerging computing paradigms for big data. *Chinese Journal of Electronics, 26*, 1–12.
9. Hung, S.-C., et al. (2016). Architecture harmonization between cloud radio access networks and fog networks. In *IEEE Access* (Vol. 3, pp. 3019–3034).

Index

F. Hussain, *Internet of Things*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-3-319-55405-1