SURVEY OF IOT COMMUNICATION PROTOCOLS

xFlow Research

Survey of IoT Communication Protocols
Techniques, Applications, and Issues

Usama Mehboob

Qasim Zaib

Chaudhry Usama

xFlow Research Inc

Printed in Pakistan

First Printing, 2016

www.xFlowResearch.com

Contents

List of Figures

Table 1: List of Acronyms

Acronym	***Expanded Form***
3GPP	3rd Generation Partnership Project
6LoWPAN	Low-Power Wireless Personal Area Network over IPv6
AES	Advanced Envryption Standard
AP	Access Point
ASIC	Application-Specific Integrated Circuit
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
D7A	DASH7 Alliance
DES	Digital Encryption Standard
EDR	Enhanced Data Rate
GFSK	Gaussian Frequency Shift Keying
HF	High Frequency
HTTP	HyperText Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
IrDA	Infrared Data Association
ISA	International Society of Automation
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
kbps	Kilobits per second
kBps	Kilobytes per second
LAN	Local Area Network
LF	Low Frequency
LoRa	Long-Range technology
LTE	Long-Term Evolution
LWID	Long Wavelength ID
LWPAN	Low-power Wireless Personal Area Network
M2M	Machine to Machine
MAC	Media Access Control
Mbps	Megabits per second
MBps	Megabytes per second
NFC	Near-Field Communication
OQPSK	Offset Quadrature Phase-Shift Keying
PAN	Personal Area Network
POS	Point-of-Sale
QoS	Quality of Service
REST	Representational State Transfer
RF	Radio Frequency
RFID	Radio Frequency Identification
SIG	Special Interest Group
SNR	Signal-to-Noise Ratio
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

Chapter 1

Introduction

We have entered a new era of computing technology where personal computers and smartphones are not the only means of digital communication. Call it a paradigm shift, but more and more types of devices are now being connected together to form what many are now referring to as the Internet of Everything (IoE). You may have come across this term or its synonymous such as Intelligent Systems, Machine-to-Machine communication, the Internet of Intelligent Devices, and so on. Call it whatever you want, but it is happening and its potential is huge.

We look at IoT as billions of connected devices, also referred to as *things*, forming a universal global neural network that will take over many aspects of our daily lives; this has been made possible by the intelligence that embedded processing provides today.

The IoT consists of different machines and devices communicating among each other and with the surrounding environment. This generates a large volumes of data which is, then, processed and transformed into something useful and actionable, something that can *command and control* sensor and devices to make our lives easier by reducing the human involvement through intelligent devices.

IoT, encompassing many aspect of our daily lives, is being utilized

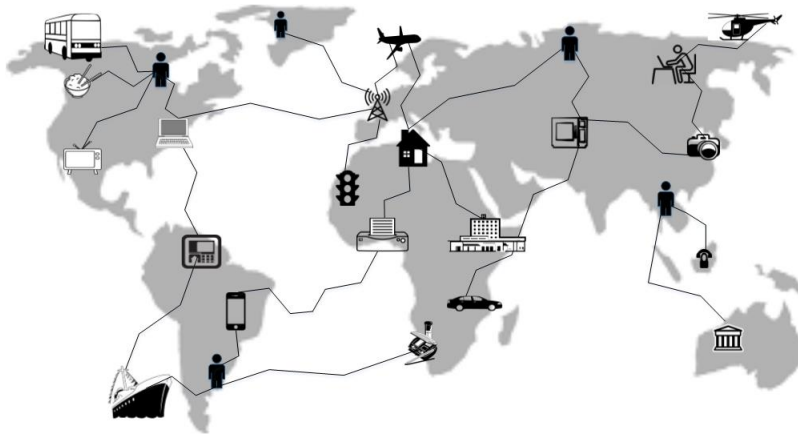

Figure 1.1: The Internet of *Things*

in multiple places including - but not limited to - connected cars and roads, automated homes, complex sensor networks in industries, and so on.

According to a forecast by Gartner[2], there will be as many as 25 billion internet-connected devices by the year 2020; it is our inherent understanding that smartphone devices might well be the *eyes and ears* of IoT applications. Some propose examples, which are less smartphone-centric, that speak of a class of devices that do not exist right now. These devices may have not been thought of yet, or are not generally considered to be 'intelligent' or connectible to the internet.

It is undeniable that IoT is slowly but surely becoming a hot topic among mainstream public. Many new product definitions are now reflecting the concept of IoT, the least of which are home automation implementations. If you have seen the 1970s hit cartoon series *The Jetsons*, then you will perhaps appreciate how the underlying concept has been around for some time but is only now being realized.

Estimates of the IoT market size in the future vary, but most ex-

perts [2] agree that it has the potential to dwarf many other markets. Today, the smartphones and PCs are considered the ultimate and pervasive consumer devices. Look around you, and count their number, then count the number of appliances, electrical outlets, lights, heating/AC units, windows and doors; which might, one day, be controlled by one of these computing devices. You will quickly realize how the IoT market has the potential to grow exponentially.

1.1 Motivation of the Book

IoT is not a new concept, and has been realized ever since the introduction of internet-enabled mobile devices. But it has taken on a fast track and has rapidly evolved in recent years with advancements in technology. Encompassing a wide range of protocols and mechanisms, it is an ever-growing field of technology, paving the way for endless possibilities.

Since IoT is a broad concept, it is especially difficult for beginners to get grasp its primary principles. In view of this tendency among the newly initiated, this book attempts to explain the very basics of IoT and the networking methodologies used; building on these concepts, the text proceeds to explain some advanced protocols that are used in IoT networks. The idea is to discuss the basics of some crucial IoT communication protocols in a single place and give the readers a starting point, from where they can go on to explore other facets of this diverse field.

Individuals or businesses interested in building automated systems and wireless sensor networks, can benefit from this book by acquainting themselves with the existing knowledge on the subject, as well as use of the tools to design such systems. In this book, we discuss the utilities and pitfalls of using each communication protocol, so the readers can weigh each option in terms of its pros and cons and adopt an approach best suited to their needs.

1.2 Organization of the Book

This book has been organized into three sections. The first section eases the reader into the concept of IoT. The idea is to provide a brief overview of IoT and explain its utility and usage in daily life.

Section two explains the basic ideas that encompass the IoT, and lays down the basis for understanding the context in which IoT is applied and used. It explains the idea of cloud networking and how it is used in the context of IoT. It then goes on to describe some limitations of

using the cloud for connected devices, and introduces a new, relatively lesser known concept known as Fog Networking which is used instead of, and sometimes in conjunction with cloud networks.

Section three comprises the main core of the book. IoT is a broad concept that encompasses a wide range of communication technologies, protocols and mechanisms. Section three is divided into four subsections that categorize the different communication protocols based on the type of functionality they provide in the protocol stack. These secions are; Physical layer protocols, link layer ptorocols, network layer technologies and application (data) layer protocols. Since it is sometimes not feasible to build complex IoT topologies over wired networks, this book majorly focuses on wireless communications.

Chapter 2

Networking in IoT

2.1 Introduction to Cloud Networks

At the very basic level, cloud computing means storing and retrieving data over the internet instead of a hard disk on a computer. Programs and data stored on a hard disk are referred to as local storage or local computing. Local computing ensures an easy and quick access to the data and it is due to this reason that it is sometimes preferred. It has been the way computers have worked since their inception and is something we all understand. Local computing also refers to computers connected to a local network, and the assorted storages attached.

For operations to fit the basic definition of *cloud computing*, there has to be some data transfer over the internet. Cloud services such as Dropbox, Google Drive and Microsoft's OneDrive have led some people to believe that the *cloud* merely refers to online storage, but cloud is so much more than just that. It involves data transfer to and from a client over the internet, it involves data synchronization between various devices over the internet, data processing on the server end and the transfer of processed data to the client over the internet, and so on. So, with just an online connection, cloud computing can be performed anywhere, anytime. For this reason, cloud computing is sometimes also referred to as *on-demand computing*.

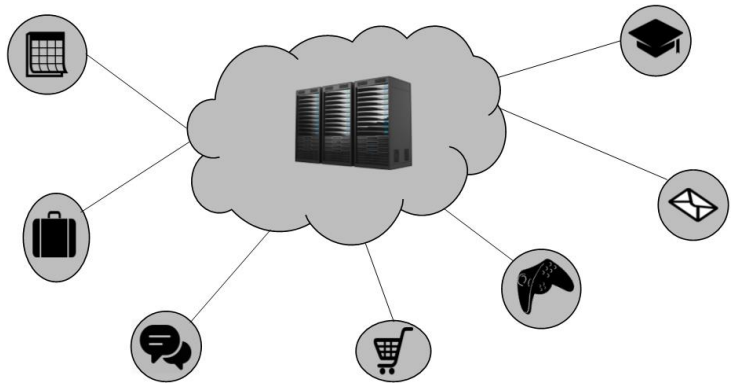

Figure 2.1: Cloud computing

Cloud computing is focused on utilizing the maximum potential of shared resources. These resources are not only shared by multiple clients but are also reallocated dynamically and on demand. For example, a cloud storage application may allocate more resources to one part of the world during peak hours, and shift those resources at night to another part of the world.

Moving to the cloud can allow companies to avoid the upfront costs of setting up an infrastructure, thus enabling them to focus on projects that add value to their business with cost and time effectiveness. Furthermore, through easier maintenance and manageability, it also allows them to get their applications running faster with flexibility and more agility.

For its many virtues, cloud computing has taken on an accelerated demand among businesses. Vendors offering cloud services are growing at a rate of more than 50 percent annually [1], which goes on to say how quickly this technology is set to overtake all other markets.

What is the significance of the cloud in IoT? cloud could potentially power a wide range of IoT applications. The low computation requirement on the client side and the high availability of data anywhere on

the internet make it ideal for a lot of use-cases. Large amounts of data can be collected through swarms of sensors deployed at the client side. This data is aggregated and sent to the cloud and is subjected to analysis for executing smart decision.

2.2 Introduction to Fog Computing

Traditional cloud models used today are incompatible with the sheer amount of volume, variety, or velocity of data that the IoT generates. Billions of previously unconnected devices are generating more than two exabytes of data each day. An estimated 25 billion *things* will be connected to the Internet by 2020 according to a forecast by Gartner [2]. Moving all the data from these 'things' to the cloud for analysis would require vast amounts of bandwidth.

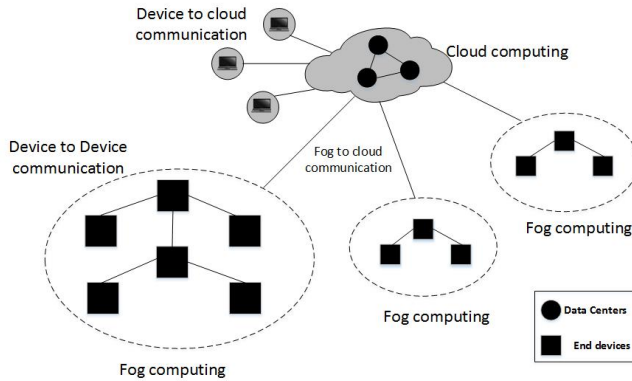

Figure 2.2: Fog Computing

The Internet of Things (IoT) is generating an unprecedented volume and variety of data. However, by the time the data makes its way to the cloud for analysis, the opportunity to act on it might already be lost. In order to counter this problem, a new type of computing - named Edge or Fog Computing - is used to act and analyze on IoT data . The concept of Edge or Fog computing includes:

- Analysis of the most time-sensitive data at the network edge, close to where it is generated instead of sending vast amounts of IoT data to the cloud
- Policy-based action on IoT data within milliseconds
- Sending the data to the cloud for long-term storage and time-based (historical) analysis

These billions of new things also represent countless new types of things. Some are machines that connect to a controller using industrial protocols, not IP. Before this information can be sent to the cloud for analysis or storage, it must be translated to IP.

Fog networks extend the functionality of the cloud to make it faster and more feasible for devices that produce or act on IoT data. Such devices, termed as fog nodes, can be deployed where there is an active internet connection. This could be on top of a cellphone tower, inside an industrial complex, along a railway or road track in the form of a beacon, or even a moving vehicle. Any device that has computing capability in addition to storage and network connectivity can act as a fog node. Such examples include routers, switches, industrial controllers, embedded servers, video surveillance cameras, and so on. IDC estimates that the volume of data analyzed on devices that are physically close to the IoT is approaching 40 percent, which is hardly surprising as analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the network.

How do Fog and cloud networks work together to enable IoT applications?

- Real-time feed reception from an IoT device using a specified protocol.
- Running of IoT-enabled applications for analysis and control in real-time with the least possible delay.
- Provide short-term storage.
- Send periodic data summaries to the cloud.

The cloud platform:

- Collects and aggregates data from various fog nodes.
- Performs analysis on the IoT data for business analysis.
- Sends insightful application rules to the fog nodes based on the analysis performed.

Fog Computing: Extending the cloud closer to the things that generate and act on data benefits the business in the following ways:

- Greater business agility: With the right tools, developers can quickly develop fog applications and deploy them where needed. Fog applications program the machine to operate in the way each customer needs.
- Better security: Protect your fog nodes using the same policy, controls, and procedures you use in other parts of your IT environment. Use the same physical security and cybersecurity solutions.
- Deeper insights, with privacy control: Analyze sensitive data locally instead of sending it to the cloud for analysis. Your IT team can monitor and control the devices that collect, analyze, and store data.
- Lower operating expense: Conserve network bandwidth by processing selected data locally instead of sending it to the cloud for analysis.

Fog computing gives the cloud a companion to handle the two exabytes of data generated daily from the Internet of Things. It accelerates awareness and response to events by eliminating a round trip to the cloud for analysis. It also avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. Fog computing also protects sensitive IoT data by analyzing it within the confines of company walls. Ultimately, organizations that adopt fog computing gain deeper and faster insights, leading to increased business agility, higher service levels, and improved safety[12].

2.3 Machine-to-Machine Communication

As the name suggests, Machine-to-Machine (M2M) communication involves data communication between two or more machines or entities without any human intervention. Typically, this is realized in applications that involve sensors, actuators, assets and information systems. Sensors such as temperature, pressure, sound sensors are mounted onto assets such as cars, vending machines, and other consumer electronics. The integration of these different devices and their communication with an information system allows for automatic process execution based on the data that has been collected and then analyzed - all without human intervention.

A very basic example of such M2M communication can be found within an air-conditioning unit inside a home. A sensor monitors the temperature of the room. When the temperature rises, the sensor senses the change and sends a signal to an actuator, which then communicates with a mechanical device - a compressor - to turn it on and thus regulate the room temperature.

The figure below demonstrates how machine-to-machine communication is carried out without any human involvement. Data is collected from consumer devices (end devices) and relayed through an M2M gateway. The data is transmitted through a cellular or internet connection and sent server-side machines for analysis. The application software processes it into meaningful information that is then sent back to end devices for performing actions.

The definition of M2M communication is relevant for both one-way and two-day communication between devices. Here are some of the key features of M2M communication.

- M2M devices generally have a low mobility, and they are expected to move rarely, if at all, and that too within a defined region.

- The transfer of data within M2M devices is defined within specific time periods.

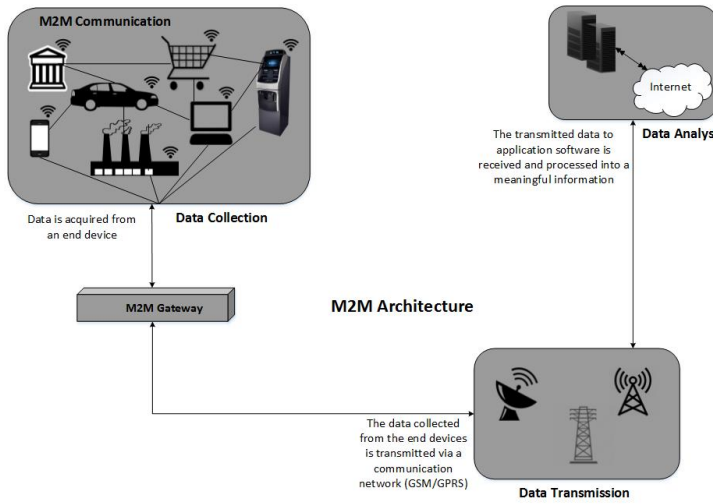

Figure 2.3: Machine-to-machine communication

- Small online data tramsmissions
- High availability of the system is warranted by a low power consumption.
- M2M devices typically use location specific triggers.
- Their use is mostly for tracking and monitoring purposes.

Chapter 3

Communication Technologies

With the rapid advancement towards IoT, an increasing number of appliances from industries to personal electronics are going to be connected to the Internet. This will cover a broader variety of use-cases in numerous environments and with varied requirements. Today, a wide variety of technologies can be used for IoT. These technologies use different communication protocols and frequency bands. In addition, these technologies offers different layer of functionalities in their protocol stack. This makes it quite a challenge to choose the best wireless technology for any IoT application.

In this section, we review the wireless technologies available for IoT, providing guidelines for selection by discussing their technical concepts and engineering pitfalls of the right technology for divergent operations.

3.1 Physical Layer Technologies

The Physical layer is the most basic and essential layer in any communication model. In this section, we will focus only on technologies that only provide without any other functionality in the protocol stack. These technologies are used with other supplementary protocols to provide full protocol stack functionality.

3.1.1 Powerline Communication

Technology Description:

Powerline communication (PLC) is a communication technology that uses AC/DC powerlines as its communication link. The data travels over powerlines, thus allowing the existing powerline infrastructure to be used for the purpose of communication without adding new wires. With the rapid growth in technology, PLC is also experiencing boost in its applications and has entered into different segments of the market which includes – but not limited to– smart grid, energy metering, lighting control, electric cars, and so on. The global agenda of energy conservation is driving the demand for intelligently communicating devices, having capability of data transmission with least power consumption.

PLC does not require additional infrastructure; thus, enabling swift deployment of smart technologies for energy management. Since the communication is done through powerlines, PLCs are not hindered by limitations encountered by wireless technologies such as short transmission range and the need for a line-of-sight.

A communication system normally consists of four major components:

- Transmitter
- Receiver
- Communication medium
- The signal itself

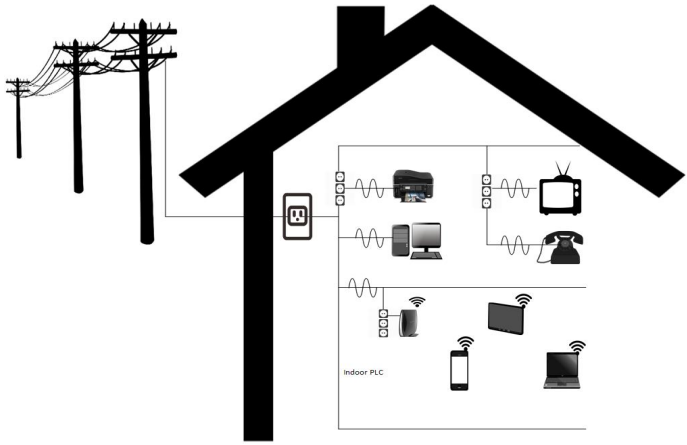

Figure 3.1: Overview of Powerline communication

As mentioned earlier, the communication medium in PLC is the powerline. Transmitter component is responsible for modulating and injecting signal into the powerline. Receiver component is responsible for demodulating the signal and retrieving data from the opposite end of link. For proper transmission of signal, the impedance should match, otherwise the signal will get attenuated as it travels to the receiver. The signal moving through the powerline is prone to noise which, in turn, can corrupt the signal.

Applications:

PLC has been widely used in niche areas as described:

- PLC has been used in automobiles for the transmission of video, music, and data over direct current (DC) circuitry.

- *Ethernet over power* is a type of PLC, used to provide Ethernet connections over AC lines, in homes, to connect computers and smart devices.

Pros:

- Use of PLC network ,in homes, eliminates the overhead of dedicated broadband cables and routers.

- Unlike Wi-Fi, PLC's signal strength reduces much less with distance. In addition to that, PLC adapters can be used to provide hot-spot in every room; thus, providing seamless coverage for all the devices.

Cons:

- Electrical connection in circuits and wiring, if not done properly, would affect negatively the powerline communication - causing interrupts and loss of signal.

3.1.2 LoRa

Technology Description:

This is proprietary LPWA technology that typically operates in unlicensed spectrum i.e. ISM band. While the physical layer of LoRa is proprietary, the rest of the protocol stack, known as LoRaWAN, is kept open, and its development is carried out by the LoRa Alliance, led by IBM, Actility, Semtech, and Microchip.

As exemplified in Fig 3.3, the LoRa network is deployed in accordance with star-of-stars topology, in which the leaf nodes (end devices) are connected to one or multiple LoRa gateways, via a single-hop LoRa link. The gateways are connected, over standard IP protocols, to a network server (NetServer). The technology employs a spreading technique, according to which a symbol is encoded in a longer sequence of bits, thus increasing the signal-to-noise (SNR) and interference ratios required for correct reception, without changing the frequency bandwidth of the wireless signal. LoRa technology has made it possible to provide variable data rates, that offers a trade-off between throughput and coverage range or energy consumption[4].

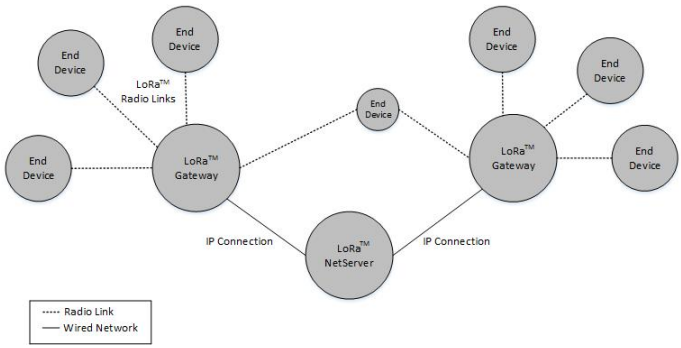

Figure 3.2: Overview of LoRa Architecture

Applications:

LoRa offers three type of devices, each intended for different purposes.

- *Class A* (for all) Devices are designed to be deployed for monitoring applications; where a centralized controlling entity would accommodate the data generated by all leaf nodes.
- *Class B* (for beacon) Devices are synchronized with the Net-Server to receive commands from a controller to perform a specific function. Examples include actuators and switches etc.
- *Class C* (continuous listening) devices keeps the receive windows always open and operates without any strict constraints on energy requriements. Examples are devices connected to power grids.

Pros:

- Ability to trade-off between range and data rate, allows the devices to work in harsh environment with least data rate but robust link connection owing to spreading technology.
- Greater Area can be covered with less gateways compared to cellular networks[4].

Table 3.1: Specifications of LoRa

Specification/feature	LoRa support
Frequency range	ISM band 868 MHZ 915 MHZ
Data Rate	$<$ 10 kbps
Channel Bandwidth	$<$500 KHz
Coverage	$<$11 km
Energy need	Low
Battery Life	$>$10 years

Cons:

- Use of gateways for communicating with end devices might cause a bottleneck due to a single point of failure.
- LoRa operates in un-licensed band which puts a limitation of 1% on duty cycle. Consequently, LoRa lack predictability as the protocol have many variable frame length, transmission time is data-rate dependent when the data-rate is controlled by the network, not the device.

3.1.3 Sigfox

Technology Description:

Sigfox is a pioneer in LPWA technology and was introduced in IoT market since 2009 and growing since. Sigfox, like LoRa, is proprietary and offers much less data rate - about 100-1000 times less than other IoT technologies. Sigfox devices uses ultra-narrowband modulation while the network level protocols are proprietary. This technology is being developed by Sigfox, aiming to deploy a controlled network dedicated to IoT, much like a cellular network. The solution for the customer is to employ Sigfox certified transmitter in the devices; data transmitted by the device is first routed to Sigfox server to scrutinize for integrity and security of the data; following which, it is routed back to applications's IT network. So user is given more ease in collection of the data from devices deployed.

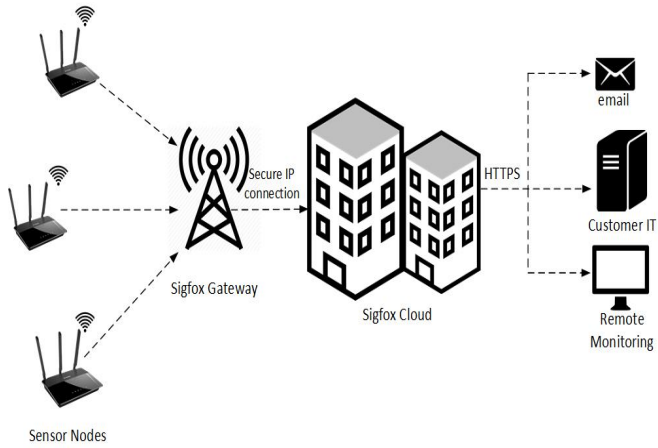

Figure 3.3: Overview of Sigfox Architecture

Applications:

Sigfox provides a unique global cellular connectivity solution, from the customers' devices to their software applications. Sigfox devices are designed to capture markets like agriculture and environment, automotive, buildings, consumer electronics. Customer is required to purchase a subscription from Sigfox certified local cellular operator and they can deploy the smart embedded devices – connected all over the internet.

Table 3.2: Specifications of Sigfox

Specification/feature	**Sigfox support**
Frequency range	Unlicensed 900 MHz
Data Rate	$<$ 100 bps
Channel Bandwidth	$<$100 Hz
Coverage	$<$13 km
Energy need	Very-Low
Battery Life	$>$10 years

Pros:

- Extremely low data rate (100 bps) offers good sensitivity in long range communication spanning multiples of kilometers.
- Sigfox claims that each gateway could handle up-to millions of connected devices and covers an area of 30-35 km rural while 3-10 km urban.

Cons:

- Sigfox doesn't implement any collision avoidance, fair use, and listen-before-talk mechanism. Consequently, multiple Sigfox devices working in ultra-narrowband could offer worst kind of interference for any wide-band system in the locality.
- A very low data rate is not practical for many devices. For example with 100bps, it takes 1.2 seconds for a mere 12 bytes payload.
- Currently deployed Sigfox devices offers one way communication without acknowledgment. Achieving reliability in this scenario requires redundant transmission that might prove inefficient for resource constrained devices.
- In order to operate on ultra-narrowband, devices are required to be equipped with precise temperature compensated crystals which costs more than regular devices.

3.2 Link Layer Technologies

Link Layer technologies are used for data transfer among adjacent nodes in a local area network (LAN). Link Layer is used for medium access control for all devices in LAN, as well as implementation of collision prevention mechanisms in data frames.

This section describes IoT technologies that provide support of link layers in their stack. Rest of the layers have been implemented by the users and companies.

3.2.1 WAVIoT

Technology Description: The WAVIoT a Narrow-band Fidelity (Nb-Fi), is an innovative, new communications technology which is designed for wide-area, low-power, machine-to-machine communication. Instead of using open source Long range technology (LORA), it uses a proprietary protocol Nb-Fi, built from scratch, for low power wide area networks (LPWAN). As a result, WAVIoT narrow-band systems provides to a greater degree of adjacent channel interference as compared to LORA Technology and more efficient spectrum utilization. Its range can span up-to 10km urban while 50km rural.

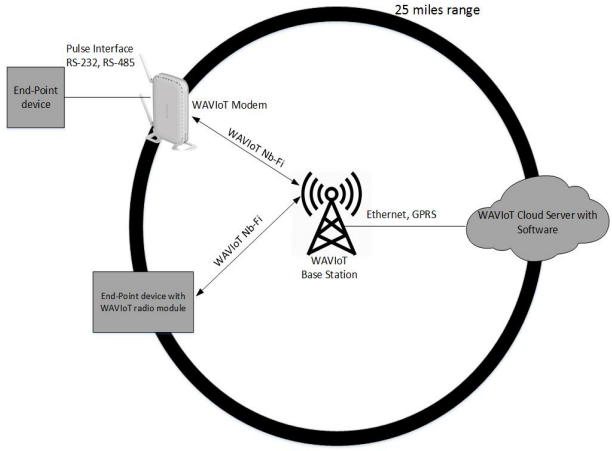

Figure 3.4: Overview of WAVIoT communication

Applications: WAVIoT has designed applications ranging from smart water meters, smart grids,irrigation, parking devices in automobiles, access control locks etc.

Pros:

- WAVIoT technology, offers long range data transfer of upto 50km (rural), which makes it suitable to use in large scale distributed IoT networks.

Table 3.3: Specifications of WAVIoT

Specification/feature	WAVIoT support
Frequency range	915 MHz, 868 MHz, 433 MHz.
Data Rate	50-100 bps
Channel Bandwidth	50 Hz
Coverage/Range	10 km urban, 50 km rural
Energy need	low (including startup)
Battery Life	20+ years

- WAVIoT, works with end nodes transmitting data to the base stations; which transfers it to WAVIoT server and saves in web-based cloud. This allows the end users to observe all readings and data over web portal.
- More protection against neighborhood channel noise and efficient spectrum utilization as compared to LORA technology.

Cons:

- High cost- being a proprietary technology, it might result in high expenditure if deployment is done on a large scale area, as all the devices would have to be purchased from a single vendor - WAVIoT.

3.2.2 DASH7

Technology Description:

DASH7 Alliance Protocol (sometimes referred to as D7A) is a wireless network protocol based on RFID technology, and its use in smart devices is proliferating. DASH7 provides a small protocol stack, a low latency with high range and a multi-year battery life for connecting moving things.

There are four different device classes defined in D7A (Dash7 Alliance Protocol).

- Blinker: It only transmits and does not use a receiver.

- EndPoint: It can transmit and receive the data. It also supports wake-up events.
- Subcontroller: It is full featured device. It is not always active. It uses wake on scan cycles similar to end points.
- Gateway: It connects D7A network with the other network. It will always be online. It always listens unless it is transmitting.

D7A describes fully functional RFID tags. All the devices in Dash7 network support one or more of the above mentioned device classes. DASH7 supports two communication models: pull and push.

The dialogs between tags and interrogators are query-response based (referred to as pull model). This request-response mechanism is described by the D7A Query Protocol. Data transfer initiated from the tags to the gateway, on the other hand, is based on the push model. This approach is implemented an automated message or a beacon which is sent on specific time intervals. This system is called Beacon Transmit Series.

DASH7 defines two types of frames: a foreground frame and a background frame. The foreground frames are regular messages which contain data or data requests. Background frames on the other hand are very short broadcast messages. Background frames are used by the D7A Advertising Protocol for rapid ad-hoc group synchronization.

Applications:

Dash7 is used in a variety of situations, owing to the fact that its signal propagation characteristics allow it to penetrate obstacles. This makes it ideal for use in smart energy and building automation applications. DASH7 also finds its uses in the development of location-based services with the help of a range of devices that are DASH7-enabled. Such devices include smartcards, watches, digital tickets, and other such products that can be built cheaply, have a small footprint and run on low power.

Table 3.4: Specifications of DASH7

Specification/feature	DASH7 support
Standard	ISO/IEC 18000-7
Frequency range	433, 868 and 915 MHz bands
Data Rate	167 kbps
Multi-hop capability	Yes, 2 hops max
Coverage	2 km
Security	AES 128-bit shared key encryption
Energy need	Very low

DASH7 is also being used for tracking purposes, such as monitoring the whereabouts of shipping boats and containers, trucks, railway carriages, and other such supply-chain assets. DASH7 is very popularly used for building large sensor networks spanning a very large area.

Pros:

- Short frequency band allows the signals to penetrate obstacles such as walls, making it less prone to disruptions
- Very low energy requirement makes ideal to be used with low-power devices
- Low cost

Cons:

- DASH7 can't handle high bandwidth data transfers, thus limiting its use to mostly sensor and actuator networks

3.2.3 Wi-Fi

Technology Description:

Wi-Fi is, without question, the most popular form of wireless data communication in use today. The Wi-Fi technology is based on the IEEE 802.11 standard, designed to replace the 802.3 Ethernet standard, and is intended to provide internet connectivity through access

points inside homes, offices, schools, and more recently in public places such as coffee shops, airports, bus terminals (even inside trains and buses).

Wi-Fi adapters are already integrated into all new smartphones, tablets, laptops and other such mobile devices. With a vast deployment of Wi-Fi infrastructures inside homes, offices, schools and public places, it is only logical to assume that Wi-Fi will provide internet connectivity to a majority of IoT *things*.

Wi-Fi networks are typically designed in a star topology, with various devices connecting to a single Access Point, which then operates as a gateway. Like Bluetooth, Wi-Fi networks operate in the 2.4 GHz band. Hence, the signals from a Wi-Fi Access Point are prone to obstruction through walls and doors. Due to this, most Wi-Fi Access Point devices are high-powered in order to provide consistent coverage throughout the building. Sometimes dual antennas are used to avoid multi-path conditions and to introduce signal diversity for better coverage.

Although Wi-Fi networks can also operate in the 5 GHz band, providing higher data rates, the effective range is much lower and hence are rarely used. 2.4 GHz Wi-Fi signals cannot, and are not meant to cover, a large area in the first place. Due to the large resource requirements of Wi-Fi (storage, memory and processing), it was only possible to integrate Wi-Fi adapters to laptops and smartphones with powerful microprocessors. However, advancement in silicon device technology has enabled it to be built into much smaller devices such as thermostats and other home appliances.

Wi-Fi can be quite power hungry for some devices that run on small batteries. But most of these devices do not even need the high data rates that Wi-Fi offers. Therefore, by compromising between data transfer rate and battery life, a clever power-management design can be implemented with advanced sleep and fast on/off protocols. Indeed, since the past few years, such protocols are being implemented into small devices, providing them with internet connectivity and making them more useful.

Taking advantage of existing infrastructure: most organizations already have a Wi-Fi infrastructure covering extensive areas of real estate. Adding more clients and applications is already a day-to-day activity, and given that IoT-based applications often involve infrequent transmissions and/or limited amounts of data, the additional load is unlikely to be much of a concern in most cases. Also note that many enterprise IoT applications will simply be new applications running on smartphones and similar devices that are already connected to the Wi-Fi network. Wi-Fi offers major advantages in capacity, coverage and ease of use.

Scalability: Increasing Wi-Fi coverage and capacity will be required for some time.

In the short term, 802.11ac largely addresses this need. Upgrades are now well under way in many shops; IoT devices based on 802.11ac will increasingly appear in the market, and backwards compatibility with 802.11n will pick up any slackers.

But bear in mind that the IEEE standards folks are also hard at work on 802.11ah, which extends the standard to the sub-1GHz spectrum, offering improved propagation (and thus range) for low-bandwidth applications. And the 802.11ad standard has already unlocked the vast amount of spectrum at 60 GHz, which offers the potential for virtually unlimited capacity (almost 7 Gbps) with somewhat restricted range. Wi-Fi offers access to more spectrum, the basic commodity essential to wireless success, than any other radio technology.

A number of Wi-Fi-based IoT products are available today, and many more will arrive in the near future. The good news is that network operations managers and staff need only worry about scale, rather than about having to learn about and support yet another radio technology.

Applications:

Wi-Fi has largely been used as a replacement for Ethernet to provide internet connectivity to handheld or mobile devices through various

access points. These access points are set up inside homes, offices, schools and colleges, shops, public places, transport terminals, buses and trains, and so on. Wi-Fi adapters are built into smartphones, laptops and other such mobile devices.

More recently, Wi-Fi modules are being built into much smaller devices such as thermostats, health trackers, watches, and so on to enable automation and to provide a means of communication for data collection and analysis over the cloud.

Table 3.5: Specifications of Wi-Fi

Specification/feature	**Wi-Fi support**
Band	2.4 - 5.9 GHz
Data Rate	54 Mbps
Coverage	50-100 m
Energy need	High

Pros:

- Security: Wi-Fi has perhaps the most robust security available in any wireless technology today, and Wi-Fi chipsets provide transparent implementations.
- Wi-Fi has a very simple setup and multple clients can connect to an access point at the same time depending on the maximum allowed as specified by the device or its settings
- Wi-Fi offers very high data rates and hence has become the standard for providing wireless internet connectivity in places around the world.

Cons:

- Wi-Fi hotspots require a lot of power and hence need a constant energy source.
- Wi-Fi adapters and their drivers require memory and processing resources that simple appliances cannot support.

- Wi-Fi signals are prone to obstacles and cannot go through walls without losing their strength
- Wi-Fi is limited by its range to within a building only.

3.2.4 WiMAX

Technology Description:

WiMAX is a wireless technology intended for high speed data communication applications by providing a low cost alternative for cable and data subscriber link (DSL). It's based on IEEE 802.16 standard[14].

WiMAX provides the data rate comparable to cable rates and has the ability to maintain a dedicated link for each subscriber. Many telephone operators desire that it is going to replace their legacy wired links. WiMAX can be used in variety of applications due to its higher data rates and longer coverage area. It can act as a backbone for Wireless LAN (WLAN) technology to connect them to the internet. Anyone with WiMAX enable devices can directly connect to the world by communicating with the WiMAX stations, without any need of intermediate link; while subscribers not having WiMAX enable devices have to connect to WiMAX station with an intermediate link of IEEE 802.11.

The behavior of WiMAX depends on the frequency ranges it operates, it normally operates in two frequency ranges, which are 11-66 GHz (High frequency range) and below 11 GHz (low frequency range). The devices have to be in sight while operating in high frequency band, providing data rate of 124 Mbps in this range – much larger than 70 Mbps data rate in low frequency band where line of sight doesn't matter.

WiMAX operates in license as well as unlicensed bands. Following four bands in the range of 2-11 GHz are very attractive:

- 2.5 GHz Multichannel-Multipoint Distribution Service (Licensed)
- 3.5 GHz Band (Licensed)

Table 3.6: Specifications of WiMAX

Specification/feature	**WiMAX support**
Frequency range	2-11 GHz
Band	20-28 MHz
Data Rate	124 Mbps
Coverage	30-50 km
Security	168-bit Digital Encryption Standard
Energy need	High

- 3.5 GHz Band (Unlicensed)
- 5 GHz Band (Unlicensed National Information Infrastructure)

While designing WiMAX security is kept in mind knowingly that it is going to be run in public networks. For that purpose, all data transmitted via WiMAX is encrypted; using the same technique which is used by most of the secure VPNs; which is 168-bit digital encryption standard (3DES). To further increase the security in WiMAX, there is a plan of using Advances Encryption Standard (AES) as future technique.

Applications:

WiMAX is mostly used by internet service providers as a replacement for their wired networks, providing internet connectivity to home users and business corporations.

Pros:

- Long range
- Bandwidth is symmetrical over long range
- Hundreds of users can be served from a single WiMAX station
- Operate on an unlicensed spectrum of frequency

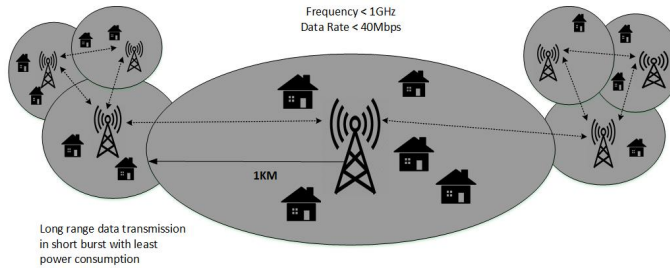

Figure 3.5: Overview of 802.11ah communication

Cons:

- Serving lots of clients results in poor bandwidth
- Service can be effected by Weather conditions
- High latency
- For longer range, the device has to be in the sight
- Signal is prone to distortion due to noise

3.2.5 802.11ah

Technology Description: IEEE 802.11ah is sub-1GHz 802.11 Wireless LAN operating in ISM band. Demand for sub-1GHz WLAN arose to meet the growing number of IoT devices; hence the IEEE task group was assigned to standardize the sub-1GHz WLAN, aiming to address the concerns regarding a large number of IoT devices requiring long range data transmission in short burst with least power consumption. IEEE 802.11ah has overcome the limited range of traditional 2.4 and 5 GHz Wi-Fi, owing to the enhanced penetration and propagation of sub-1GHz radio waves. 802.11ah brings the Wi-Fi to cover places like building, attics, back yards, malls, and garages as well, by infiltrating better through obstructions and walls.

Table 3.7: Specifications of 802.11ah

Specification/feature	802.11ah support
Frequency range	915 MHz, 868 MHz, and 433 MHz.
Data Rate	100 kbps - 4000 kbps
Channel Bandwidth	variable (4,8,16,26 MHz)
Coverage	1 km (outdoor)
Energy Needs	Low-Medium
Battery Life	depends on the hardware power constraints

Applications: Devices on 802.11ah technology are being produced for smart grid, home automation, low power sensors, wearable consumer electronics etc.

Use Cases: 802.11ah is used in large offices and venues to provide flexible light control. It has also been used to extend the network coverage in university campuses.

Pros:

- Owing to the enhanced propagation and penetration of 900MHz radio waves, coverage of one hop transmission range would be longer; thus, requiring less devices in single network
- 802.11ah devices offer much less power consumption because of efficient physical layer design with low power medium access control(MAC) protocols; thus, requiring smaller frame formats. The protocol also offers policies for prioritized traffic from sensors in a network.
- Linking of IEEE 802.11ah access points and gateways together e.g. as a mesh network to server as back-haul connection; thus, accommodating the aggregated traffic produced by all individual nodes [15].

Cons:

- IEEE 802.11ah supports wide range of data rates on variable spectrum bandwidth. Increasing the data rate would lessen the range and battery power.
- Lack of standard worldwide frequency - Different country/regions have different frequency specifications. For example, in China, it is 780 MHz. European standards define it to operate at 868 MHz, whereas a band of 915 MHz and 950 MHz is used in USA and Japan respectively.

3.2.6 Bluetooth

Technology Description:

Bluetooth was introduced in 1994 by telecom vendor Erickson as a wireless communication standard for interaction between computers and mobile phones. Initially, it fell under the IEEE 802.15.1 standard, but that is no longer the case. The standard is now being controlled by Bluetooth SIG.

Bluetooth has been a huge success in mobile phones and other such handheld devices. Today, almost all mobile phones irrespective of their features or cost offer basic Bluetooth connectivity. Bluetooth was widely adapted because it allowed hands-free wireless Bluetooth connectivity for mobile calls. And now with the advancing capabilities of smartphones, Bluetooth is finding more and more use-cases, such as high-quality music streaming, health and fitness tracking, and so on.

Bluetooth is ideally intended to replace short-range wired communication. Although used typically in a point-to-point or star topology, the Bluetooth specification also includes more complex topologies. Bluetooth is designed to consume low power, and hence is typically mounted in low-powered devices with small rechargeable batteries.

The Bluetooth standard includes application profiles as well, which describe how applications are going to exchange information and perform a particular task. For example, you have the A/V Remote Profile

which defines how multimedia playback (audio and video) is controlled through the use of a Bluetooth remote control. Bluetooth owes its excellent interoperability to the comprehensive certification programs as they are defined by Bluetooth SIG, and which cover everything from the protocol stack to the application profiles.

Applications:

How is Bluetooth related to IoT? Bluetooth finds its uses in a lot of day-to-day applications. It connects wireless accessories to a smartphone or tablet acting as a gateway. A phone-controlled garage door opener and a heart-rate monitor tracking your heartbeats and sending them to a health application on your smart-phone, are all examples of IoT applications running over Bluetooth.

Table 3.8: Specifications of Bluetooth

Specification/feature	**Bluetooth support**
Frequency	2.4 GHz
Data Rate	2.1 Mbps
Coverage	10-100 m
Energy need	Low - Medium

Pros:

- Widely used standard makes it convenient to connect to various devices
- Cost effectiveness means it can be implemented into low-end devices as well
- Very easy and convenient to use
- Free to use

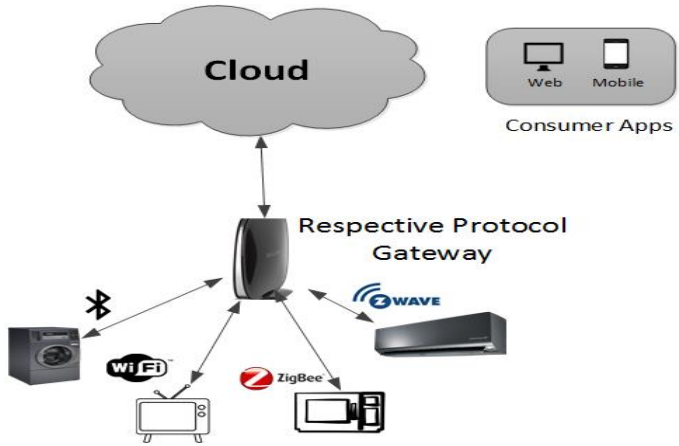

Figure 3.6: Short-range household communication technologies

Cons:

- Security concerns - devices can be hacked into easily
- Bluetooth installed into many devices today allows only one ongoing connection at a time
- Bluetooth is limited in its range, ideal only for communication within a room. More range require a lot more power

3.2.7 Bluetooth Low Energy (BLE)

Technology Description:

Bluetooth Low Energy (BLE) has very recently been added to the Bluetooth specification. Sometimes also referred to as 'baby bluetooth', BLE is designed for lower data rates and low power consumption, thus enabling it to operate on low-powered devices that can run for upto two years before being charged.

Aside from the name, BLE is very different from standard Bluetooth and the two are not compatible. BLE has some very specific use-cases that involve small data transfer and a very low power consumption.

BLE devices come in two different modes. Single mode or Bluetooth Smart, and dual mode or Bluetooth Smart Ready. Also considering classic Bluetooth BR/EDR, there are three different types of Bluetooth devices in use today. Unfortunately, they are not inter-compatible, which makes it important to specify beforehand which version of Bluetooth is to be used in a device.

Despite the lower specifications, BLE offers an improved coverage over classic Bluetooth, which is due to an increased modulation index. Despite the fact that it can support a range of up to 200 feet and more, BLE's ideal applications mostly require short-range communication.

Classic Bluetooth supports a maximum of eight devices connected simultaneously in a star topology. The BLE specification removes this limit, however, and can support unlimited number of connections - at least theoretically. The practical limit, however, is between 10 to 20 devices.

Applications:

BLE has rapidly accelerated the growth of the Bluetooth market and is now supported by a new generation of mobile devices. The applications enabled by BLE range from file transfer between devices, hands-free smartphone connectivity, health and fitness tracking, to even industrial applications that use it for communication and automation.

Thanks to the newly introduced proximity capabilities, BLE can now be used to run location-based services as well, which include - but are not limited to - geo-fencing and radio beaconing.

Table 3.9: Specifications of Bluetooth Low Energy

Specification/feature	BLE support
Frequency range	2.4 GHz
Data Rate	1 Mbps theoretical, 10 kbps practical
Coverage	50 m
Energy need	Very low

Pros:

- Lower energy consumption paves the way for more possibilities as Bluetooth Low Energy can now be used with more, lower-powered devices.

Cons:

- Keeping in mind the low energy requirements, BLE is limited in its bandwidth capability and provides a slightly lower transfer rate.

3.2.8 WiBree

Technology Description:

WiBree communication protocol is a short range protocol to implement significant amount of bluetooth functionality with less power; thus, complimenting the Bluetooth. The Wibree is specially useful in applications where Bluetooth communication is not possible for being an unreliable protocol or where the data rates are not very demanding because WiBree is a standard with data rates as lower as three times than Bluetooth 2.0[8].

A group headed by Nokia is dedicated for setting the specifications of WiBree which includes semiconductor manufacturers, vendors and service providers. WiBree can operate with either a dual-mode or a standalone chip. For communicating at larger ranges, dual-mode Wibree is used; at low power demands, standalone chip is utilized. Some of the fundamental characteristics of Wibree protocol include

device discovery, reliable point-to-multipoint data transfer, ultra-low power operation and encrypted communications[6].

Wibree fulfills the demand for a radio technology that:

- allows data transmission between Bluetooth devices and small button-cell battery devices
- results in a minimal addition to size and cost of Bluetooth devices such as mobile phones and PCs
- creates low cost and smaller in size options for devices such as small battery devices

Applications:

WiBree is a technology for communication between small devices from different vendors. It can be built into products such as sports sensors, wireless keyboards and watches, which can then connect to host devices such as personal computers and mobile phones. It is essentially the missing communication link between small battery devices and host devices.

The advantage of Wibree over Bluetooth that makes it ideal for small battery operated devices is that it is less costly and a lot more power efficient than Bluetooth.

Table 3.10: Specifications of WiBree

Specification/feature	**WiBree support**
Frequency range	2.5 GHz
Data Rate	1 Mbps
Coverage	10 m
Energy need	Very low

Pros:

- Wibree is designed to consume very small amounts of power and hence is ideal for use in small devices, typically wearable gadgets.

Cons:

- Owing to the fact that it is designed for low power consumption, Wibree is limited in its bandwidth and low data transfer rates.

3.2.9 RFID (Radio-frequency identification)

Technology Description:

Radio-frequency identification, often shortened to RFID, is the use of electromagnetic fields for data transfer between two devices without a direct physical connection while being in sight of each other. RFID technology is particularly important in context of IoT because it is being realized in a large number of industrial applications for tracking and monitoring supply-chain and logistic goods through the use of RFID tags.

A typical RFID system consists of three components.

- An RFID tag is lodged into or attached to an item that is to be tracked. This tag contains information about the item.
- An RFID interrogator which handles communications with RFID tags. This is typically deployed into scanners, POS terminals, and so on.
- A back-end system that maintains a database and links it to RFID interrogators.

RFID operates in three frequency bands:

- Ultra-High Frequency
- High Frequency
- Low Frequency

Applications:

RFID tags are well adapted for logistics and traceability applications. Depending on the requirement and circumstances, different frequencies are used for a variety of applications such as luggage tracking, pet and livestock tracking, ID cards for authorization on terminals, and so on.

Table 3.11: Specifications of RFID

Specification	RFID support	
Frequency range	LF	30 KHz - 300 KHz (134 KHz typical)
	HF	3 - 30 MHz (13.56 MHz typical)
	UHF	300 MHz - 3 GHz (850 - 960 MHz typical)
Data Rate	LF and HF	4-10 kbps
	UHF	Upto 640 kbps (40 kbps on average)
Coverage range	LF	10 cm
	HF	10 cm - 1 m
	UHF	15 m
Energy need	Low	

Pros:

- RFID tags are inexpensive and can be deployed easily on a large scale
- Varying frequency bands allow for easy adaptability to the requirements

Cons:

- RFID systems can be easily disrupted
- RFID tags may collide with each other causing ambiguities and data inaccuracy
- There are a lot of security concerns with RFID technology, as your tags can be easily read without your knowledge. There have been cases of identity theft with tag duplication

3.2.10 Near Field Communication (NFC)

Technology Description:

NFC is a secure, short-range communication standard for interaction between two electronic devices wirelessly. Unlike many other wireless communication, connections are established without requiring any prior set-up. NFC allows users to make connections simply by touching the devices together, thus enabling them to make transactions and access digital content.

NFC is a form of Radio Frequency Identification, but it has its own set of standards that govern its interface and operation.

Applications:

NFC is mostly used for transactions on point-of-sale terminals, banks, shopping malls, and so on. The applications range from monetary to navigation and even authentication.

Table 3.12: Specifications of NFC

Specification/feature	NFC support
Frequency range	13.56 MHz
Data Rate	424 kbps
Coverage	4-10 cm
Energy need	Low-Medium

Pros:

- NFC transactions are inherently more secure, considering that the two devices need to be in very close proximity to each other, eliminating risks of spoofing or ID duplication without the user's knowledge
- Not only do the NFC standards define a contact-less operating environment, they also describe other specifications such as data rates and data formats. Hence, standardized equipment from a wide range of manufacturers and vendors can be used together.

Figure 3.7: NFC Communication Network

- NFC transactions require no prior set-up or configuration, making it more convenient for users and vendors alike

Cons:

- NFC is limited by its range, and is prone to disruptions as it requires very close proximity. equipment (such as Smartphones) with NFC require special designs and are expensive.

- NFC is widely used for electronic transactions such as shopping, bill payment and so on, making it an ideal target for hackers who can exploit vulnerabilities and hack a system using only their phones

Table 3.13: Specifications of RuBee

Specification/feature	RuBee support
Frequency range	131 kHz
Data Rate	9.6 kbps
Coverage	1-30m
Energy need	Very low

3.2.11 RuBee

Technology Description:

Rubee, also known as long wavelength ID (LWID), is peer to peer protocol that uses magnetic waves instead of radio waves as a mode of communication. Rubee is an evolved form of radio frequency identification. This protocol was well acclaimed in radio technology and received Frost and Sullivan award in 2007 and later standardized as IEEE 1902.1.

Rubee's magnetic waves work at low frequency of 131 KHz which lead to far less power consumption than traditional high frequency devices.

Rubee's compliant devices are less power hungry, and low cost as compared to RFID counterparts. Rubee's reading ranges are far greater than traditional RFID owing to the use of volumetric loop antennas. Ranges estimates from 10-20 feet to as high as 10,000 square feet.

Applications:

Rubee produces non-detectable range limited magnetic signal; it is used at sites where ultra-most security is required especially where other modes of communication i.e., ZigBee, RFID, and Wi-Fi are not allowed. Rubee find its use in several inventory tracking applications, especially military devices.

Pros:

- Long battery life - Rubee compliant detectors and devices uses extremely low data rate and low frequency that offers us low power consumption and maximum battery life (upto 15 years).
- Human Safe - A RuBee signal's energy ranges are in nanowatts. These low frequency signals cannot be absorbed by living tissues; plus, it does not affect implanted devices like pacemaker.
- High security and privacy - Rubee finds its use in high security sites. The eavesdropping range is limited as well as the tag range. If someone needs to listen to the tag conversation, they must be in close proximity, which puts the intruders at a great risk.
- Less Noise - Rubee devices are less susceptible to extraneous noise.

Cons:

- Rubee's disadvantage lies in less data rate and packet size. IEEE 1902.1 has standardized Rubee at 1200 baud though protocol could be implemented with higher baud rate with less range. Packet size is limited to tens to hundreds bytes that is acceptable for most applications.

3.2.12 EnOcean

Technology Description:

EnOcean is a wireless energy harvesting technology. EnOcean – compliant devices employ energy converters which reap power from surroundings by harnessing temperature differences, light energy, and mechanical motion. It delivers high data rate at low energy consumption without any use of batteries. It takes care of multiple simultaneously transmitting devices; these devices, each playing a specific role, in homes and offices could be run for years without worrying about battery power and maintenance. More than about 50 manufacturing companies have already created about 200 EnOcean compliant products.

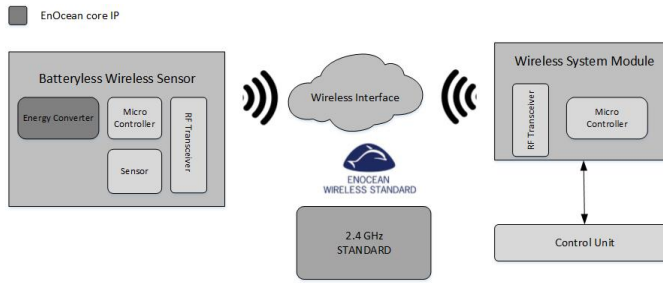

Figure 3.8: Overview of EnOcean communication

Since most energy harvesters deliver only very small amounts of power, it is necessary to accumulate energy over time, while the system is sleeping, and to lose only a small fraction of it in the process of radio communication. Therefore they have an extremely low idle current [7].

Applications:

EnOcean devices are particularly useful for short-range, less data-heavy applications; for example, door-locks in buildings, acquiring sensor data over short area.

Use Cases

IQmat is the mattress with integrated pressure sensors, specially designed to ease out the stress on nurses in care department. Nurses has to deal a lot of stress in care department by looking after the old patients. The maintenance-free sensor, designed on EnOcean technology, senses the change in pressure and sends the sms alerts to nurses that parent has left the bed.

Table 3.14: Specifications of EnOcean

Specification/feature	EnOcean support
Frequency range	868.3 MHz or 315 MHz (Worldwide)
Transmit power	6 dBm typical. at antenna input
Data Rate	125 KBps
Coverage/Range	30 meters (Indoor) 300 meters (Outdoor)
Channel Bandwidth	280 KHz
Energy need	extremely low (including startup)

Pros:

- EnOcean, being self-powered technology, offers huge advantages for IoT infrastructure in remote and inaccessible places by eradicating the need of battery replacement and regular maintenance.

- EnOcean-technology compliant devices offer indoor transmission range of upto 30 meters today.

Cons:

- Low throughput- In congested areas, with multiple EnOcean devices, an increased collision rate may causes a drop in throughput. This limitation is discussed in [13].

3.2.13 Cellular

The emerging market of IoT offers a huge opportunity to employ the already in-use ubiquitous cellular networks for machine-to-machine communications. There is a competition between the telecom operators and alternative IoT technologies i.e., ZigBee, Wi-Fi, and Bluetooth to capture the expending IoT market. In order to use existing cellular networks for IoT solutions, some constraints related to IoT like low cost, high battery life need to be addressed.

There are multiple technologies that were introduced for cellular networks.

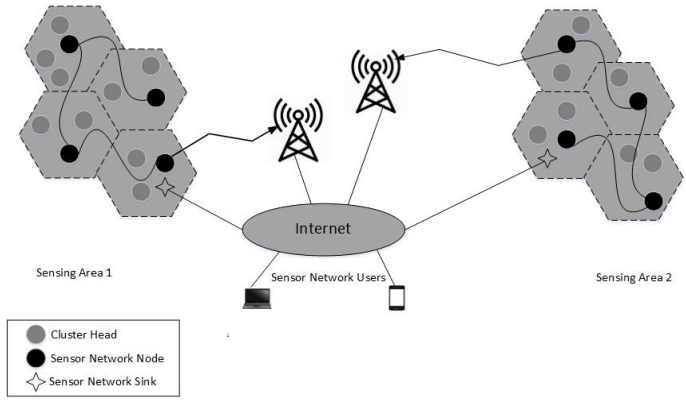

Figure 3.9: Overview of Cellular communication

LTE-M and NB-LTE-M:

Traditional LTE standard has 100 Mbps downlink rate, which demands a lot of energy and power consumption. Most IoT devices don't need higher bandwidth and data rate; this led to a new cellular IoT standard LTE – designed for least power consumption, cost effective and longer battery life. The move to LTE is inevitable and encompasses all devices connected to the Internet – ranging from the highest speed smartphone to the lowest speed utility meter or wearable device. LTE 3GPP release 12 focused on low cost of LTE-M with higher capacity; while release-13 focused on further optimizations leading to *narrow band LTE-M (NB-LTE-M)* . This release-13 standardized the LTE-M with up-link and down-link data rate of 200 kbps, apart from reducing the device bandwidth to 200 KHz. LTE-M compliant devices operate with specifications like low power consumption (running up-to 10 years with AA devices), while not leaving the mark of data security, interoperability, easy installation and wider coverage.

Applications:

Cellular IoT applications can be found in remote areas where deployment of an additional IoT network would not be possible due to limited access. A particular use-case can be smart-metering

Table 3.15: Specifications of Cellular

Specification/feature	LTE-M support
Frequency range	7-900 MHZ licensed Band
Data Rate	<150 kbps(NB-LTE-M) <1Mbps(LTE-M)
Channel Bandwidth	NB-LTE-M(200 KHz) LTE-M (1.4 MHZ)
Coverage	<15 KM (NB-LTE-M) < 11 KM (LTE-M)
Energy Need	Low-Medium
Battery Life	>10 years

Pros:

- Unlike other low power wide area (LPWA) proprietary technologies (Sigfox, LoRA), LTE-M is a standardized technology which operates in licensed band, which means more throughput and less interference[11].
- Narrow band offers low cost both on the device side and baseband. The device can be manufactured with low cost RF equipment; thus, easing the consumer as less power is spent on data transmission for narrow band baseband.
- Re-usability of existing cellular spectrum. LTE-M can be deployed on existing cellular networks either by re-framing one GSM channel or by multiplexing with guard bands in existing LTE.

Cons:

- Cellular data-plan for end devices might prove costly, especially on large scale deployment involving hundreds of sensors.

3.2.14 Weightless

Technology description:

Weightless is the name given to a new set of Low-Power Wide-Area Network (LPWAN) technology standards for Machine-to-machine data communication. This is realized in the form of base stations that are

connected to thousands of client machines, much like cellular technology. However, these standards have been defined to provide a wider coverage while reducing the power requirements at the same time. The transmission overheads are kept minimal for devices that need to exchange only a few bytes of data, hence the name *Weightless*.
The Weightless standard is being defined and controlled by the Weightless Special Interest Group (SIG). So even though the protocol is open, it can be considered proprietary because patents are only issued to devices that qualify the standard's requirement.

Applications:

The Weightless technology is geared towards low-cost M2M applications which require a wide coverage with minimal power usage. Such applications include smart metering and energy-related communications, automation and monitoring of transport facilities, tracking of goods at POS terminals, warehouses and industrial setups, security and surveillance, and so on.

Table 3.16: Specifications of Weightless

Specification/feature	**Weightless support**
Frequency band	Sub-giga ISM Band (<1 GHz)
Data Rate	1 Kbps - 1 Mbps
Coverage	5 km
Energy requirement	Ultra low

Pros:

- Low cost devices: Weightless devices are expected to be inexpensive, and each single chip is expected to cost around 2 USD.
- Very low power consumption: A battery life of upto 10 years is expected for the connected devices.
- Wide-Area coverage: Countrywide coverage is expected since a lot of applications such as smart metering will depend on it.

- Security and reliability: As per the Weightless standard, data speed or size may not be as important as its reliability and security for mission critical applications.

Cons:

- Although not really a disadvantage, Weightless does not support a high bandwidth and data rate. 4G cellular networks can provide much higher data rates.
- The standard has very stringent power consumption requirements. Hence, it is difficult for manufacturers to make such devices that qualify the requirements of the standard.

3.3 Network Layer Technologies

Network layer is supposed to transmit and route packet between two networks. The IoT technologies, which use router/gateway or have support upto network layer, are categorized in this section. These technologies, aggregate the traffic from end-nodes at gateways, which in turn forward it to servers or some other network.

3.3.1 6LoWPAN

Technology Description:

IPv6 over LWPAN (6LowPAN) was designed to connect the low power devices to internet; thus, fostering the growth of IoT. A set of standards has been defined by the 6LowPAN group like header compression and encapsulation; all these standards enable the use of IPv6 over link layer frames as defined by IEEE 802.15.4. 6LowPAN uses PHY and MAC layers of IEEE802.15.4 and IPv6 for its networking layer, as described in figure below:

Content
UDP
IPv6
6LOWPAN
IEEE 802.15.4

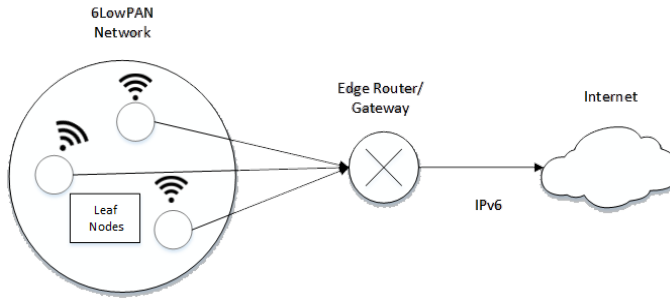

Figure 3.10: Overview of 6LowPAN

Applications:

6LowPAN are best suited for applications that require connectivity at low data rate and for devices having a lower form factor. Key applications include supervisory control, non-critical monitoring and closed/open loop control applications.

Pros:

- Use of IPv6 in proliferating market of IoT devices is unavoidable. 6LowPAN provides an open standard IPv6 protocol for low power devices and would be accepted readily.
- 6lowPAN, based on IPv6, supports stateless auto configuration; each device in 6LowPAN network is automatically assigned an IPv6 address. As devices are located in remote areas so this dynamic addressing helps in connectivity.

Cons:

- There is a need for a suitable security mechanism for transmission over 6LowPAN as AES security scheme used in IEEE 802.15.4 link layer is not secure enough to be relied upon for classified communication.
- Using 6LowPAN requires significant knowledge of IPv6 stack for

end users; it is a new standard in the market and will take sometime to catch on with its counterparts i.e. ZigBee.

3.3.2 ZigBee

Technology Description:

ZigBee is a very popular wireless networking standard for building sensor networks. It is a packet-based open and global protocol that has been designed to provide a secure and reliable communication architecture at low power. ZigBee is defined by the IEEE 802.15.4 standard and it operates in the ISM (Industrial, Scientific and Medical) radio bands[3].

The ZigBee standard is defined as a Low Rate Wireless Personal Area Network. Such networks are built to operate over short distances, transmitting small data and consuming very little power. The transmit power of each node is specified at +6 dB, with the receiver sensitivity being around -85 dBm or better. ZigBee uses O-QPSK modulation and a 128-bit AES Encryption scheme.

ZigBee networks has a 16-bit PAN ID which is assigned to each node within a single network. This allows up to 65535 networks coexisting side by side. Some networks may even share the same frequency, although that is not advisable.

Applications:

ZigBee is used in a wide variety of applications. Some of the major application profiles include:

- Smart Meters: This profile brings advanced capabilities to smart meters, including load control, pricing support, text messaging, security, and so on.
- Home Automation: Products from different manufacturers can be integrated together to fit the needs of the modern home au-

Table 3.17: Specifications of ZigBee

Specification/feature	ZigBee support
Frequency range	2.4 GHz
Data Rate	250 Kbps
Bandwidth	2 MHz
Coverage	50 m
Channels	16, non-overlapping (5 MHz separation)
Energy need	Low

tomation setup. This includes thermostat and heating, lighting control, motion sensing, security and surveillance, and so on.

Pros:

- Low power consumption
- Smart time allocation used for communications that need a fixed bandwidth, thus avoiding collisions and ensuring reliability.
- Low cost of ZigBee modules
- Low latency ($<$ 30 ms for device discovery, 15ms for wakeup and 15 ms for active channel access)
- ZigBee can be used to create large networks, and one master node can have as many as 254 devices connected to it
- ZigBee implements AES-128 for data encryption and security

Cons:

- The major disadvantage of ZigBee is its short range and low data transfer speed.

3.3.3 Z-Wave

Technology Description:

Z-Wave, a proprietary protocol promoted by *Z-Wave Alliance*, is specifically designed to transmit short messages from control unit to slave

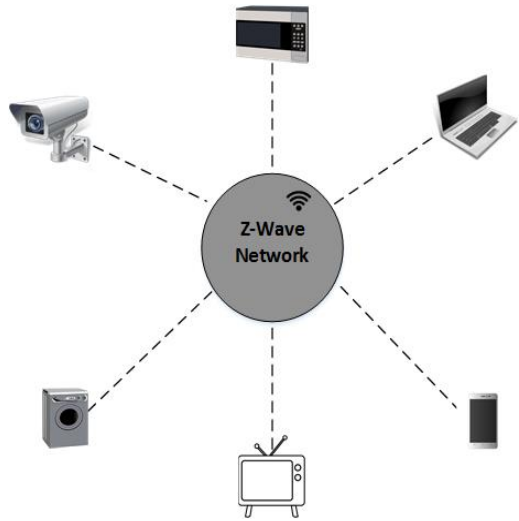

Figure 3.11: Z-Wave communication protocol

devices at minimal power consumption; this makes it particularly useful for automation in commercial and residential environments. Z-Wave is distinct from other radio communication protocols, as instead of utilizing large bandwidth, it intends to support only short burst commands i.e., on-off or raising an alarm and device meta-data[10].

Z-Wave network operates using controllers and slaves. A controller may send a message to slave which may act as monitoring devices or actuators; thus, responds and executes the controller instructions. A message in Z-Wave network may traverse upto 4 hops maximum which is suitable for house and close vicinity applications. Z-Wave network support dynamic addition of slaves i.e. sensors and routing devices.

Applications:

Z-Wave technology works best for close proximity devices i.e., electronics devices in home, entertainment systems, lights, thermostats.

Table 3.18: Specifications of Z-Wave

Specification/feature	Z-Wave support
Frequency range	ISM Bands (900 MHz, 868 MHz)
Data Rate	9.6 kbps, 70 kbps, 200 kbps
Coverage	30 m indoors and 100 m outdoor
Energy requirement	Low

Z-Wave wireless network lets the devices in hospitals and home talk to each other as well as with humans. Use of low power sub-1GHz radio waves allow better penetration through walls, basements; thus, enabling the controller to reach all the sensors and actuators in local vicinity.

Use Cases:

Z-Wave devices has been used to provide smart solutions in homes. A notable bedroom solution is worth mentioning here: by pressing a button from your smart phone, lights are shutoff, alarms are set and temperature of the room is adjusted for night.

As far as the market is concerned, Z-Wave is supported by more then 325 manufactures all around the world and there are plethora of home automation devices, to be operated in Z-Wave network, are already in the market.

Pros:

- Use of sub-1GHz radio waves cause no interference from common household devices operating in crowded 2.4 GHz band.

- Use of controller and slaves helps achieving more scalable network by dynamic addition of sensors, alarms according to the demand of buildings.

Cons:

- Procedure to add and remove devices in Z-Wave is slightly cumbersome. Removal of a device requires it to be unpaired first, detached from Z-Wave network and then removed.

- Current Z-Wave technology is not stable in the market and lots of errors and unusual behaviors are reported by customers. Devices are often seen to report errors on receiving commands from controller. At times, controllers are needed to factory reset and relearn all network topology of slave nodes.

3.3.4 Symphony

Technology Description: Symphony is an end-to-end wireless solution designed specifically for low power wide-area network (LPWAN) applications. It is built with LoRa using the IEEE 802.15.4 standard to create a new type of radio modulation. Symphony was introduced by Link Labs to provide long range M2M and enterprise solutions.

Applications: A single Symphony gateway can be used to talk to 10,000 nodes; thus, covering an entire building. Symphony also targets more battery life; a node that sends a message every 10 minutes could easily last between 8 to 10 years depending on the application. Thus, Symphony is typically used inside industrial setups or wide area sensors networks where data collection needs to be periodic and not real-time.

Table 3.19: Specifications of Symphony

Specification/feature	**Symphony Link support**
Frequency range	Sub Giga
Data Rate	$<$ 40 kbps
Coverage	1-10 km
Energy need	Very-Low

Pros:

- Real-time Advanced Encryption Standard (AES) key exchange.
- Decentralized architecture, with each gateway node doing network processing locally.
- Dynamic scheduling would allocate resources to both up-link and down-link in IoT network.
- Symphony Link is several times cheaper than cellular networks

3.3.5 Wavenis

Technology Description:

Wavenis technology was developed by Coronis systems for applications, with extremely low power battery size but needing a long-range data link. It is an extremely low-power communication technology. It offers a solution for battery-powered, autonomous devices in fixed or ad-hoc network by extending Bluetooth industry standard.

A protocol stack and a RF transceiver is the core component of this technology, providing an excellent combination of reliable and secure connections by using minimal amount of power on long range link. It illustrates high resistance towards interference and obstacles, making it widely used in products found in LAN, WAN and PAN.

Wavenis range depends on line of sight communication with range upto 1 kilometer; the use of automatic frequency control helps in achieving maximum performance for any Wavenis product. Also, it is complaint with U.S and European electromagnetic regulation standards.

Applications:

Wavenis radio technology is used in Wireless sensor networks (WSN) and in low data rate domestic and Industrial applications. Wavenis extends the Bluetooth technology and is implemented on RF architecture providing use-cases in applications for which there is no need for a direct solution. This technology provides interoperability between different networks and remove the need of a gateway; thus, reducing

the significant cost.

Wavenis, to meet the goals of designer, provides license which allow integration between ASIC, system design, low-power baseband and RF. The features offered in Wavenis license is as follows:

- Wavenis provides a flexible solutions.
- Wavenis gives ability to the designers to build their own radio interface using Wavenis ASIC.
- Wavenis gives option to the designers to use its protocol stack in their micro-controller.

Table 3.20: Specifications of Wavenis

Specification/feature	**Wavenis support**
Frequency range	433, 868, 915 MHz
Data Rate	2.4 - 100 kbps
Coverage	1km
Energy need	Low

Pros:

- Power consumption is very low
- Unit cost is very low
- Configurations are completely programmable
- Installation is very easy
- Can tolerate interference making it possible to co-exit with other technologies
- Can support multiple network topologies
- Support ongoing quality-of-service to provide reliable communications

Cons:

- Connection should be in line of sight

3.3.6 INSTEON

Technology Description:

INSTEON is a home automation technology aiming to make smart home appliances ranging from bulbs, switches to thermostats and remote controllers. This technology employs a dual-band scheme involving both radio frequency and AC power line (power line technology). It's ability to transmit on both channels (RF and power line), helps to achieve a robust and reliable data transmission. All INSTEON devices act as peers in mesh topology, i.e., each device can be a transmitter, a receiver, or a repeater for INSTEON protocol messages, without any need of router or controller. Each device is assigned a unique identifier by its manufactures which is used in similar way a MAC address is used in IP-based networks[5].

Applications:

INSTEON devices cover all the home automation related stuff. These devices include wired and wireless home appliances ranging from switches, dimmers, bulbs, thermostats, speakers, wires, door locks, sensors and security.

Table 3.21: Specifications of INSTEON

Specification/feature	**INSTEON support**
Frequency range	Radio: 900 MHz. Powerline: 132 KHz.
Data Rate	$<$ 38.4 kbps
Channel Bandwidth	$<$ 100 Hz
Coverage	$<$ 45 meters
Energy Needs	Very-Low
Battery Life	$>$10 years

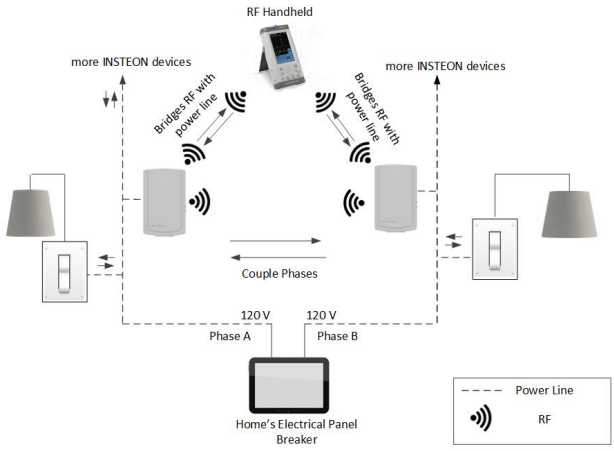

Figure 3.12: INSTEON communication Model

Pros:

- Decentralized architecture avoids single point of failure.
- INSTEON devices are deployed in homes without any central server; each device works as a repeater - sending signal to every other device to ensure reliability and strengthening of the signal.
- Each INSTEON device message is checked for errors and if error is detected a re-send is requested.

Cons:

- INSTEON, being a proprietary technology, prevents other to do research or bring innovation in the field which might put a cap on the growth of INSTEON in the market in near future.

3.3.7 WirelessHART

Technology Description:

WirelessHART, based on IEEE 802.15.4, was introduced in 2007 to address the limitations posed by Zigbee in industrial applications. Since then, WirelessHART is the most widely used communication technology among smart sensors. It's a secure, robust and self-organizing network that supports both mesh ans star topologies. It shares the physical layer with Zigbee; however, for higher layers, both technologies have their own implementations. WirelessHART network operates with four types of devices:

1. Gateway: To establish a link between controller and end nodes.

2. Network Manager: Manages the operations of network.

3. Field devices: End nodes.

4. Security Manager: Responsible for exchanging and managing the security keys.

Applications:

WirelessHART could be employed in all process field equipments. These includes events, alarms, equipment management - as well asclosed loop protocols and monitoring devices for gas, temperature, pressure and water flow.

Table 3.22: Specifications of WirelessHART

Specification/feature	**WirelessHART**
Frequency range	2.4 GHz
Data Rate	250kbps
Coverage	Indoor (30m) Outdoor (100m)
Energy need	Medium-Low

Pros:

- Devices in WirelessHART network communicate on fixed time slots, using time division multiple access (TDMA); this results in reduced power consumption and less collisions of data frames.
- Security - It's a secure and robust protocol; all messages are encrypted and authenticated on each hop. Furthermore, multi-layer security is provided by different secret keys to ensure the data integrity.
- Reliability - WirelessHART network operates on true mesh topology; means, each node can act as a router. This avoids the single point of failure, as well as, ensures the successful packet transmissions.

Cons:

- WirelessHART uses TDMA where each node has to wait for it's allocated time slot to transmit packets; this might cause a significant delay in a congested network.

3.3.8 MyriaNed

Technology Description:

MyriaNed is developed by DevLab as a communication platform for wireless sensor networks. It is developed on a contagious communication style based on standard ratio broadcasting. The interaction between humans known as gossiping is reflected in this approach. Adjoining neighbors timely send and receive messages. Each message spreads like a virus - repeated and duplicated towards all nodes that spans the network; thus, this approach is also referred to as epidemic communication. It is a decentralized communication technology where each node has equal rank in the hierarchy, and plays a role in discovering the neighbors and helping scale the network.

For the following two reasons,, this protocol is considered robust and efficient:

- The nodes, at the time of sending a message, don't need to know with whom they are connected to or who is in their neighborhood; data is shared instantaneously without any preplanned routing.
- The messages spread like a virus; the integrity of data is retained even if a message between two nodes is lost. The message from some other node, following a different route, would end up to that node - making the communication reliable

There is no need of reconfiguring the network whenever any node is added, moved or even removed from the network. The protocol used is a self-configuring solution. With this platform, nodes can exchange different type of information/messages with each other at the same time as the protocol don't require any interpretation of the content of the message the nodes has to forward; making a heterogeneous network.

The platform provides a functionality to program the software of the wireless sensor nodes over the air, enabling updates to be done on a deployed network. Functionalities and roles for nodes can be added later without the need to make changes to the base of the network.

MyriaNed has a very low energy dependency because of its low calculation power and small stack. Therefore, this platform can be run with a small battery on a simple micro-controller, reducing single node cost significantly . DevLab members work with a single chip solution in which the radio and micro-controller are integrated. This chip, with an attached battery, is smaller than a 2 euro coin.

The cost of expansion is pretty low as there is no addressing scheme needed in the network to configure; new nodes can be added in the network and these added nodes would be synchronized with the network..

Applications:

Some notable MyriaNed applications include: flexible heat and light control systems inside buildings, public transport seat reservation sys-

tems, and agriculture etc.

Use-Cases:

MyriaNed Modem Kit named EduKit has been successfully used to manage the train seats reservation system.

Pros:

- There is no limitation on numbers of concurrent nodes. Network is capable of scaling from a few nodes to hundreds of thousands.
- There is no single point of failure; messages are transmitted in distributed fashion in a robust mesh topology.
- Utilize extremely low power, as mostly the nodes are in standby mode.
- Multi-path communication makes it very reliable.

3.4 Application/Data layer Technologies

The Application layer is the top layer in the communication model, providing data to the user-level applications. This section only covers such technologies that provide application-level connectivity. These can be used in conjunction with other technologies to provide complete connectivity functionality.

3.4.1 CoAP

Technology Description:

CoAP is an application-level protocol designed for ubiquitous IoT devices being deployed in low-power lossy networks. Like HTTP, it works in a REST style but uses datagram for transmission. It uses 2 layer structure to achieve reliability: a messaging layer for asynchronous communication in UDP packets and a second layer that ensures the reliability using req/rep codes. These two layers form the CoAP header as described in the figure below[16].

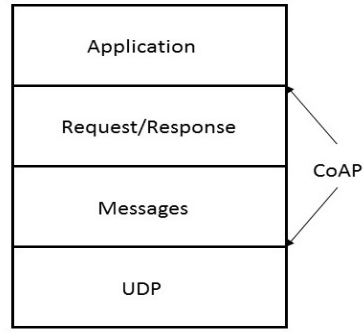

Figure 3.13: Architecture of CoAP

Applications:

This protocol is designed for nodes with constrained resources, like 8-16 bit micro-controllers having limited RAM and ROM. These kind of devices are especially used in IoT networks. Some IoT networks such as IPv6 over Low-Power Wireless Personal Area Networks (LWWPANs) or 6LoWPANs have high error rates; using CoAP in these scenarios helps achieve reliable communication over the web while minimizing the messaging overhead, and reducing the packet fragmentation thus reducing the error rate.

Pros:

- It supports large data transfer just like TCP does in HTTP by fragmenting the payloads and ensuring their right delivery order. CoAP offers a BLOCK option in which large data is transfered in chunks of request-response pairs between resources. Consequently, the server can handle this large data transfer without any connection setup.

- In Http, requests (GET) are always generated from client side to retrieve any data from server; this model is expensive for energy constrained devices. CoAP supports an OBSERVE options for clients which, if agreed between server and leaf node, would allow an asynchronous data transfer from server to all of its observers.
- Similar to Web discovery, CoAP offers a device discovery in resource-constrained devices.

3.4.2 IrDA

Technology Description:

Infrared data association (IrDA) like NFC and RFID, is categorized in last 100m connectivity relationships. The communication is done in the line of sight by two devices over the infrared spectrum. A large percentage of IoT devices would be in the vicinity of 100 meters; IrDA and other short range technologies would be useful in connecting these applications[9].

Applications:

IrDA is aimed to support close range computing devices and peripheral, single function devices like electronics business cards, and wireless sensors.

Table 3.23: Specifications of IrDA

Specification/feature	IrDA support
Frequency range	IR Light frequencies
Data Rate	9.6 kbps - 16 Mbps
Coverage	1 m
Channel	Half duplex
Energy need	Low-Medium

Pros:

- Point-to-point communication is easy

- Cost effective

Cons:

- Requires an angle of at least 30 degrees from the beam, thus it has design limitations
- Short ranged, and always requires line-of-sight for connectivity

Chapter 4

Appendix

Table 4.1: Long Range Wireless Communication Protocols

Protocol	**Range**	**Data Rate**
802.11ah	1 km	100 kbps - 4000 kbps
Wavenis	1 km	2.4 - 100 kbps
Dash7	2 km	2.4 - 100 kbps
Weightless	5 km	5 km 1 kbps - 1 Mbps
LoRa	<11 km	<10 kbps
Sigfox	<13 km	<100 bps
Cellular	<15 km (NB-LTE-M) & <11 km (LTE-M)	<150 kbps (NB-LTE-M & <1 Mbps (LTE-M)
WAVIoT	10 km - 50 km	50 - 100 bps
WiMAX	30 - 50 km	54 Mbps

Table 4.2: Short Range Wireless Communication Protocols

Protocol	**Range**	**Data Rate**
NFC	4 - 10 cm	424 kbps
RFID	10cm (LF) 10cm - 1m (HF) 15m (UHF)	4 - 10 kbps (LF & HF) Avg. 40 kbps (UHF)
IrDA	<1 meter	9.6 kbps - 16 Mbps
WiBree	10 meters	1 Mbps
Rubee	1- 30 meters	9.6 kbps
INSTEON	<45 meters	<38.4 kbps
ZigBee	50 meters	20 - 250 kbps
BLE	50 meters	1 - 3 Mbps
Bluetooth	10 - 100 meters	1 - 3 Mbps
Z-Wave	30 - 100 meters	Avg. 40 kbps
Wi-Fi	50 - 100 meters	<54Mbps
EnOcean	30 - 300 meters	125 KBps

OSI Layers	IoT Technologies	Short Range	Long Range
PHY	LoRa		✓
	Sigfox		✓
	Powerline		
Data Link	Wifi		
	WiMax	✓	
	802.11ah		✓
	Bluetooth	✓	
	BLE	✓	
	WiBree	✓	
	RFID	✓	
	NFC	✓	
	WAVIoT		✓
	Cellular		✓
	RuBee	✓	
	Weightless	✓	
	DASH-7	✓	
Network	Zigbee	✓	
	6LowPan		
	Z-Wave	✓	
	ZigBee	✓	
	Symphony		✓
	WirelessHART	✓	
	ISA100.11a	✓	
	Wavenis	✓	
	INSTEON		✓
	MyriaNed	✓	
	EnOcean		✓
Application	CoAP		
	IrDA	✓	

Table 4.3: IoT communication technologies for long and short ranges

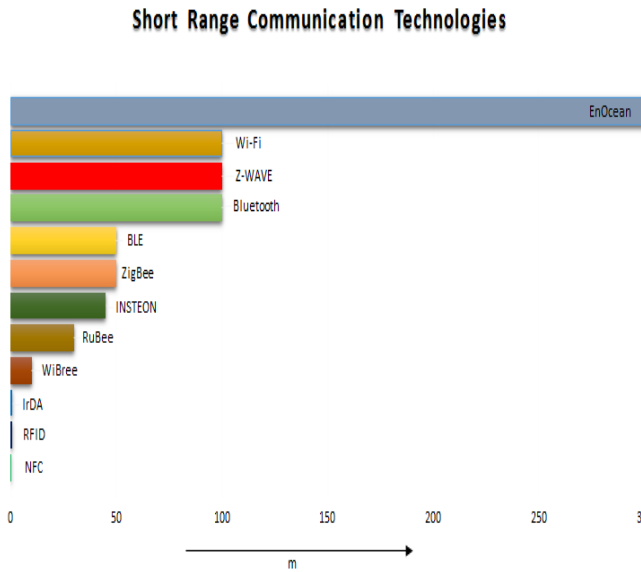

Figure 4.1: Short Range communication Technologies

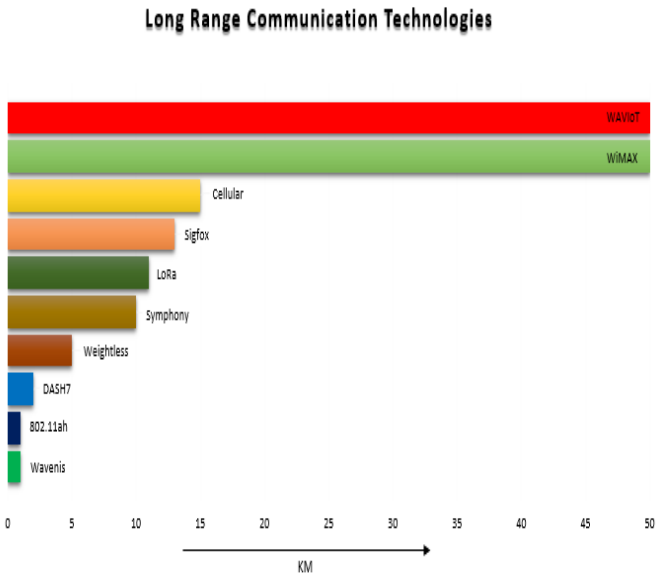

Figure 4.2: Long Range communication Technologies

Bibliography

[1] *The economy is flat so why are financials Cloud vendors growing at more than 90 percent per annum?* http://www.fsn.co.uk/channel_outsourcing/the_economy_is_flat_so_why_are_financials_cloud_vendors_growing_at_more_than_90_percent_per_annum#.UbmtsPlJPGA/.

[2] *Gartner Symposium: The Disruptive Impact of IoT on Business.* http://www.gartner.com/newsroom/id/2905717.

[3] ZigBee Alliance. Zigbee and wireless radio frequency coexistence - zigbee white paper. pages 1–15, 2007.

[4] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios. *arXiv preprint arXiv:1510.00620*, 2015.

[5] Jin Cheng and Thomas Kunz. A survey on smart home networking. *Carleton University, Systems and Computer Engineering, Technical Report, SCE-09-10*, 2009.

[6] Jimish K. Desai Nitin K. Nakum Ashita A. Brahmwar Devang G. Chavda, Gaurav N. Mehta. Wibree technology with bluetooth. *International Journal of Engineering Research and Applications (IJERA)*, 2(3), 2012.

[7] EnOcean. Enocean - the world of energy harvesting wireless technology. 16(3):1–6, 2015.

[8] Sarman G.Ranavaya. The wireless zoo and wibree. pages 1–27.

[9] Bryan J. Donoghue Kirk W. Lindstrom Stuart Williams Iain Millar, Martin Beale. The irda standards for high-speed infrared communications. pages 1–20.

[10] Musewerx. Z-wave wireless control: Technology, system and applications. pages 1–14.

[11] Nokia Networks. Lte-m - optimizing lte for the internet of things. *white paper*, pages 1–16, 2015.

[12] Cisco White Paper. Fog computing and the internet of things: Extend the cloud to where the things are. 2015.

[13] Joern Ploennigs, Uwe Ryssel, and Klaus Kabitzsch. Performance analysis of the enocean wireless sensor network protocol. In *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*, pages 1–9. IEEE, 2010.

[14] Rahul Singha Chowdhury Sourangsu Banerji1. Wi-fi and wimax: A comparative study. *Indian Journal of Engineering*, 2(5), 2013.

[15] Weiping Sun, Munhwan Choi, and Sunghyun Choi. Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz. *Journal of ICT Standardization*, 1(1):83–108, 2013.

[16] Prof. Raj Jain Xi Chen. Constrained application protocol for internet of things. 2014.