19UEC603 INTERNET OF THINGS

OBJECTIVES:

- To explain about Internet of Things.
- To impart knowledge of IoT networks and M2M Technology.
- To make students aware of security issues in application of Internet of Things.

UNIT-I: INTRODUCTION TO IoT

Definition and Characteristics of IoT, Physical Design of IoT – IoT Protocols, IoT communication models, IoT Communication APIs, IoT enabled Technologies – Cloud Computing, Embedded Systems, IoT Levels and Templates, Domain Specific IoTs – Home, City, Environment, Energy, Agriculture and Industry

UNIT-II IoT NETWORKS

Smart Objects: The "Things" in IoT: Sensors, Actuators, and Smart Objects, Sensor Networks - Connecting Smart Objects: "Communications Criteria" -Range, Frequency Bands, Power Consumption, Topology, Constrained Devices, Constrained-Node Networks. "IoT Access Technologies"- IEEE 802.15.4

UNIT-III IoT and M2M

The Vision-Introduction, From M2M to IoT, M2M towards IoT-the global context, A use case example, Differing Characteristics.

UNIT IV IoT PRIVACY, SECURITY AND GOVERNANCE

Vulnerabilities of IoT, Security requirements, Threat analysis, Use cases and misuse cases, IoT security tomography and layered attacker model, Identity establishment, Access control, Message integrity, Non-repudiation and availability, Security model for IoT.

UNIT V APPLCIATIONS AND CASE STUDY

Over view – e-health monitoring – City automation – Automotive Application – Environmental monitoring - Agricultural and commercial management.

TEXT BOOKS:

1. Vijay Madisetti, Arshdeep Bahga," Internet of Things A Hands-On-Approach",2014
2. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017.
3. Daniel Minoli, "Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications", ISBN: 978-1-118-47347-4, Willy Publications

REFERENCES:

1. Parikshit N. Mahalle& Poonam N. Railkar, "Identity Management for Internet of Things", River Publishers, ISBN: 978-87-93102-90-3 (Hard Copy), 978-87-93102-91-0 (ebook).
2. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stamatis Karnouskos, Stefan Avesand, David Boyle, "From Machine-to-Machine to the Internet of Things", ISBN 9780124076846, Academic Press 2014.

UNIT-1

UNIT-I
INTRODUCTION OF IOT

IoT comprises things that have unique identities and are connected to internet. By 2020 there will be a total of 50 billion devices /things connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data.

Definition:

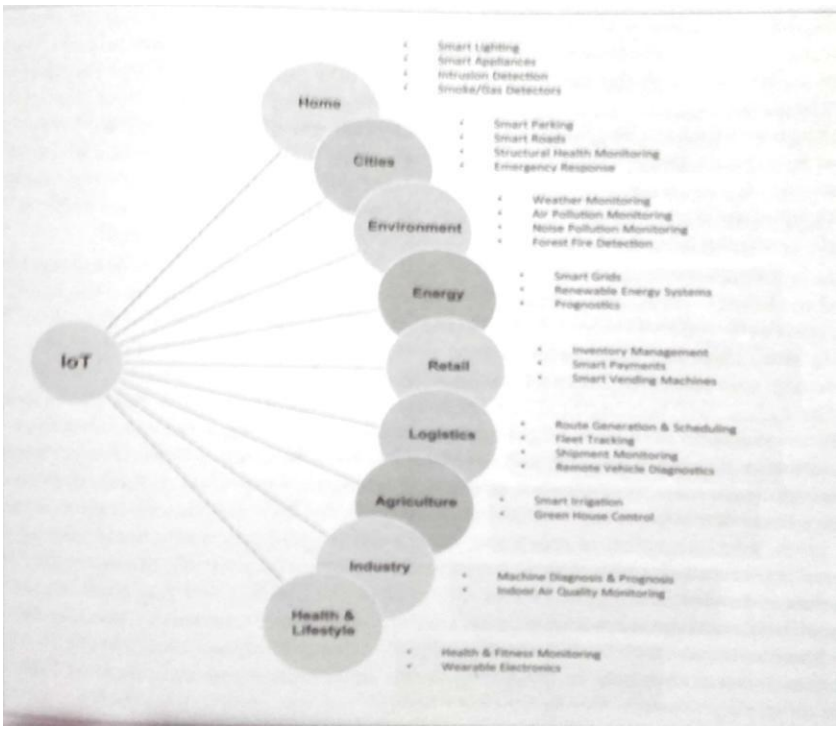
A dynamic global n/w infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual –things have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information n/w, often communicate data associated with users and their environments.

Characteristics:

1) **Dynamic & Self Adapting**: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context or sensed environment.
   Eg: the surveillance system is adapting itself based on context and changing conditions.
2) **Self Configuring:** allowing a large number of devices to work together to provide certain functionality.
3) **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
4) **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).
5) **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

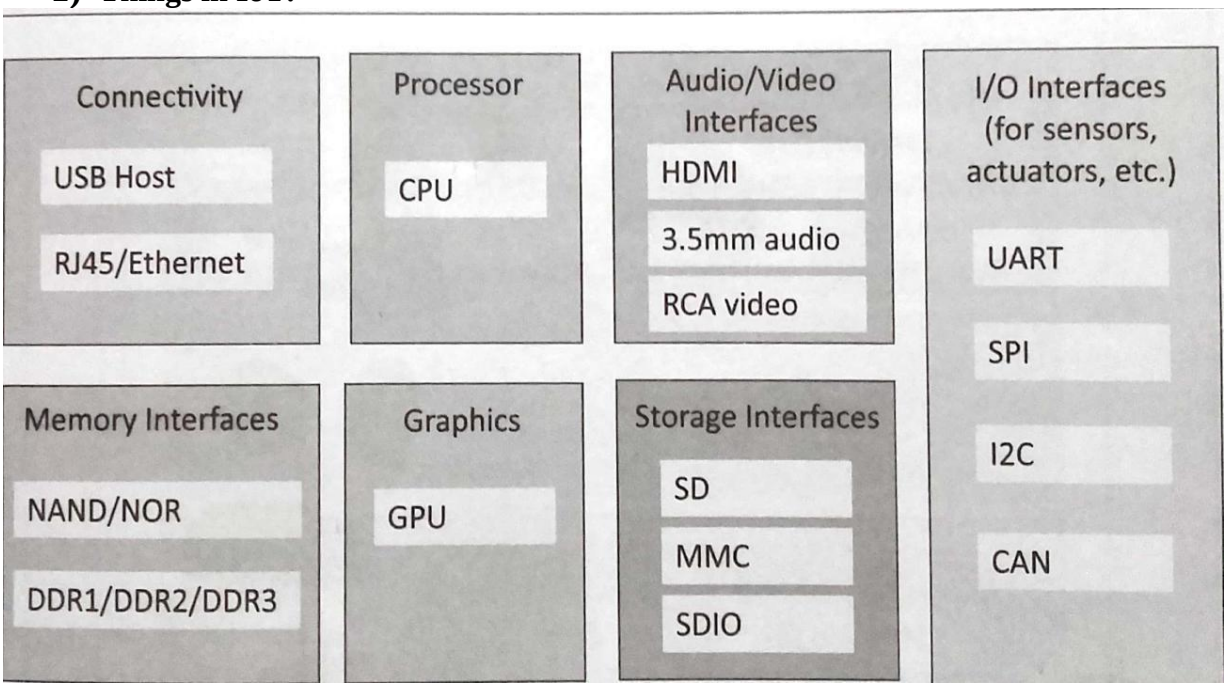
Applications of IoT:

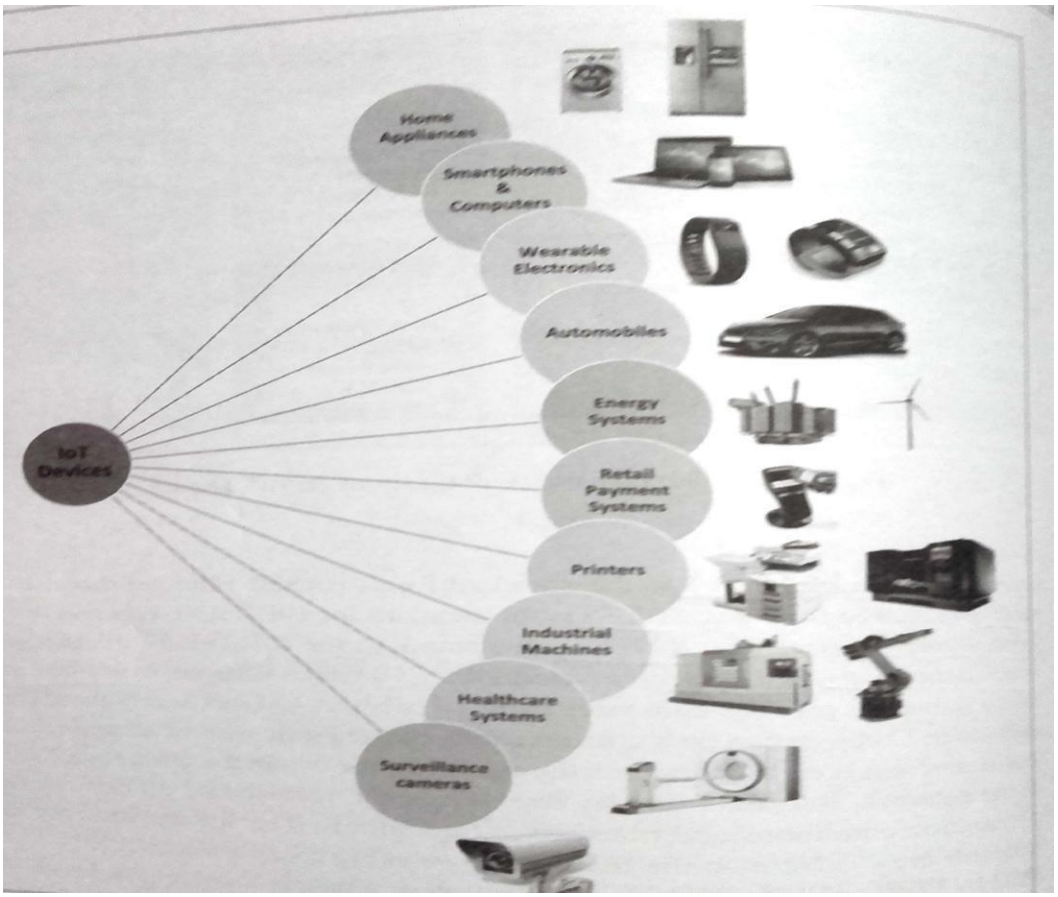
1) Home
2) Cities
3) Environment
4) Energy
5) Retail
6) Logistics
7) Agriculture
8) Industry
9) Health & Life Style



Physical Design of IoT

1) **Things in IoT:**



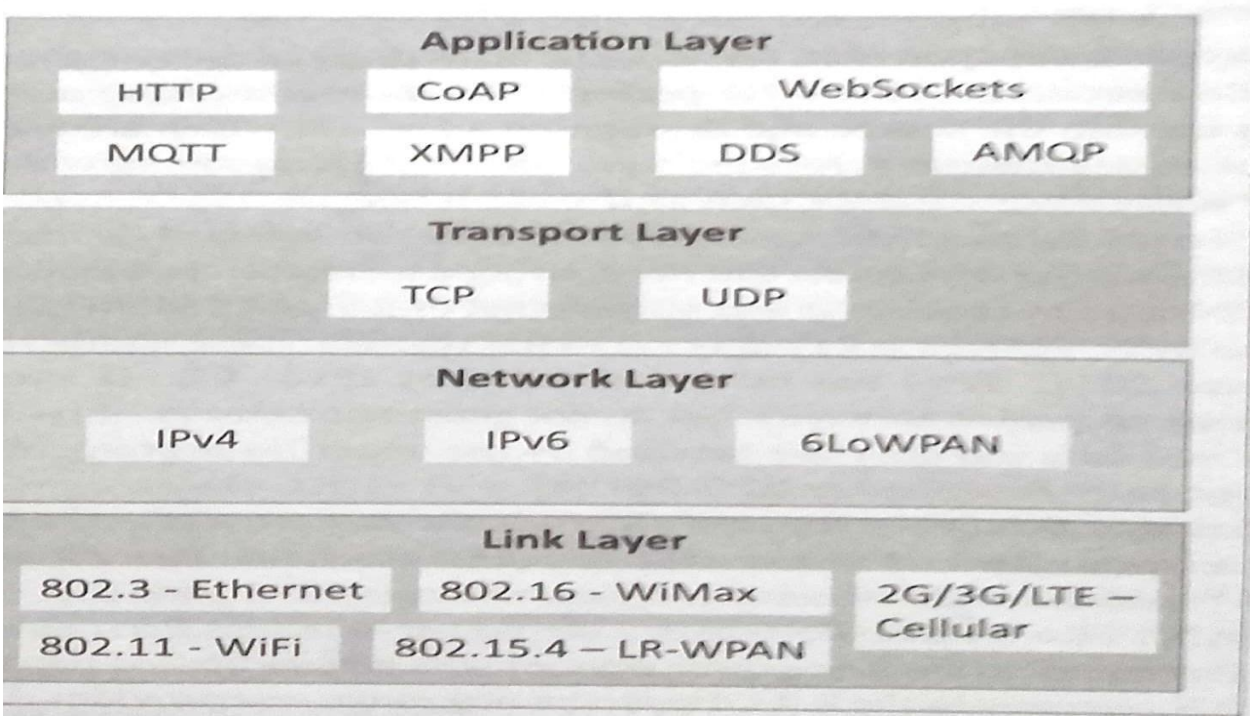


The things in IoT refers to IoT devices which have unique identities and perform remote sensing, actuating and monitoring capabilities. IoT devices can exchange data with other connected devices applications. It collects data from other devices and process data either locally or remotely.

An IoT device may consist of several interfaces for communication to other devices both wired and wireless. These includes (i) I/O interfaces for sensors, (ii) Interfaces for internet connectivity (iii) memory and storage interfaces and (iv) audio/video interfaces.

2) IoT Protocols:

a) Link Layer : Protocols determine how data is physically sent over the network‘s physical layer or medium. Local network connect to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how packets are coded and signaled by the h/w device over the medium to which the host is attached.



Protocols:

- 802.3-Ethernet: IEEE802.3 is collection of wired Ethernet standards for the link layer. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet over fiber.
- 802.11-WiFi: IEEE802.11 is a collection of wireless LAN(WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.
- 802.16 - WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.
- 802.15.4-LR-WPAN: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.
- 2G/3G/4G-Mobile Communication: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G).

B) **Network/Internet Layer:** Responsible for sending IP datagrams from source n/w to destination n/w. Performs the host addressing and packet routing. Datagrams contains source and destination address.

Protocols:

- **IPv4:** Internet Protocol version4 is used to identify the devices on a n/w using a hierarchical addressing scheme. 32 bit address. Allows total of 2**32addresses.
- **IPv6:** Internet Protocol version6 uses 128 bit address scheme and allows 2**128 addresses.

- **6LOWPAN:**(IPv6overLowpowerWirelessPersonalAreaNetwork)operates in 2.4 GHz frequency range and data transfer 250 kb/s.

C) Transport Layer: Provides end-to-end message transfer capability independent of the underlying n/w. Set up on connection with ACK as in TCP and without ACK as in UDP. Provides functions such as error control, segmentation, flow control and congestion control.

Protocols:

- **TCP:** Transmission Control Protocol used by web browsers(along with HTTP and HTTPS), email(along with SMTP, FTP). Connection oriented and stateless protocol. IP Protocol deals with sending packets, TCP ensures reliable transmission of protocols in order. Avoids n/w congestion and congestion collapse.
- **UDP:** User Datagram Protocol is connectionless protocol. Useful in time sensitive applications, very small data units to exchange. Transaction oriented and stateless protocol. Does not provide guaranteed delivery.

D) **Application Layer:** Defines how the applications interface with lower layer protocols to send data over the n/w. Enables process-to-process communication using ports.

Protocols:

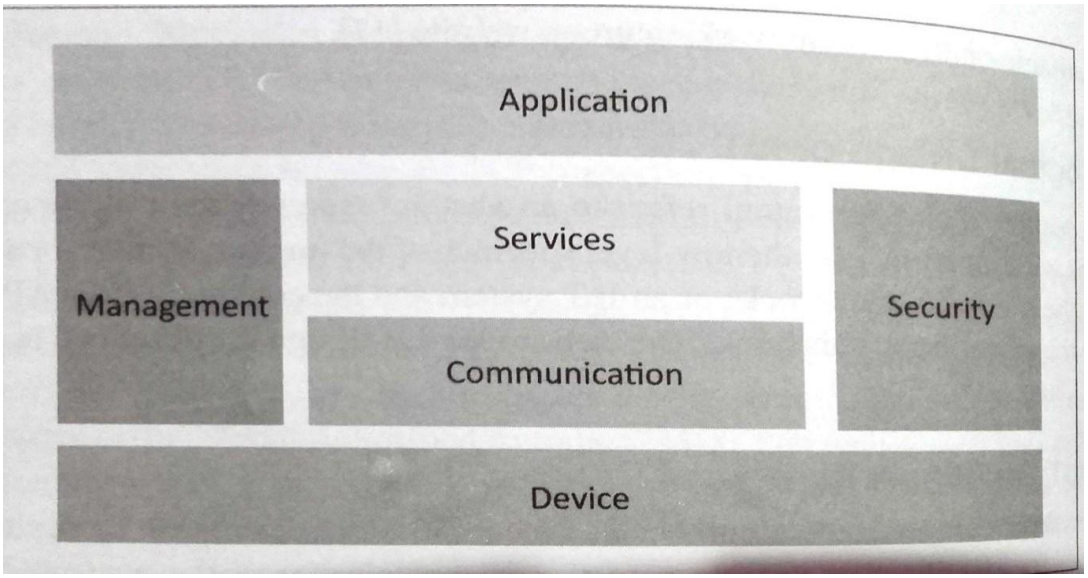
- **HTTP:** Hyper Text Transfer Protocol that forms foundation of WWW. Follow request-response model Stateless protocol.
- **CoAP:** Constrained Application Protocol for machine-to-machine (M2M) applications with constrained devices, constrained environment and constrained n/w. Uses client-server architecture.
- **WebSocket:** allows full duplex communication over a single socket connection.
- **MQTT:** Message Queue Telemetry Transport is light weight messaging protocol based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.
- **XMPP:** Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.
- **DDS:** Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.
- **AMQP:** Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

LOGICAL DESIGN of IoT

Refers to an abstract represent of entities and processes without going into the low level specifies of implementation.

1) IoT Functional Blocks 2) IoT Communication Models 3) IoT Comm. APIs

1) **IoT Functional Blocks:** Provide the system the capabilities for identification, sensing, actuation, communication and management.

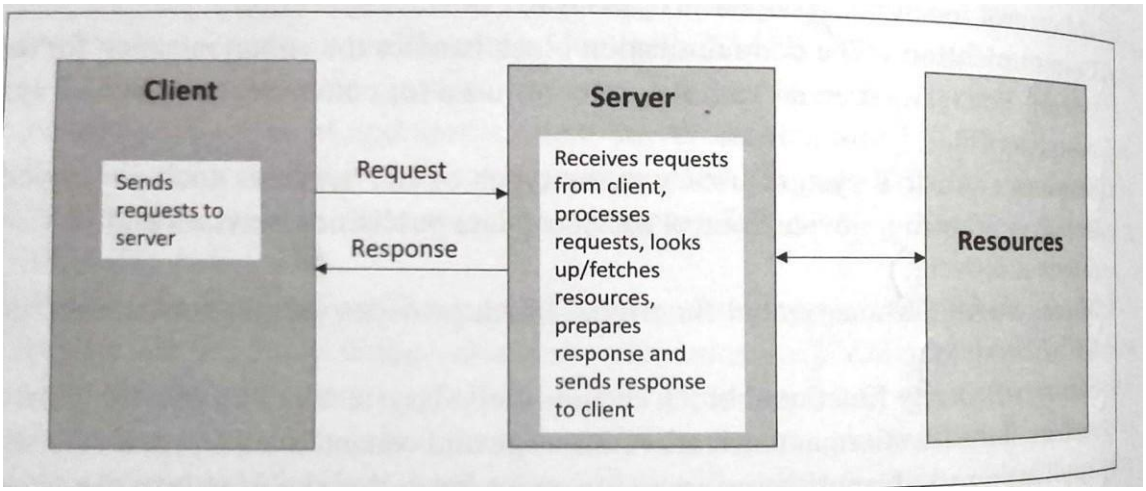


- **Device:** An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.
- **Communication:** handles the communication for IoTsystem.
- **Services:** for device monitoring, device control services, data publishing services and services for device discovery.
- **Management:** Provides various functions to govern the IoT system.
- **Security:** Secures IoT system and priority functions such as authentication ,authorization, message and context integrity and data security.
- **Application:** IoT application provide an interface that the users can use to control and monitor various aspects of IoT system.

2) IoT Communication Models:

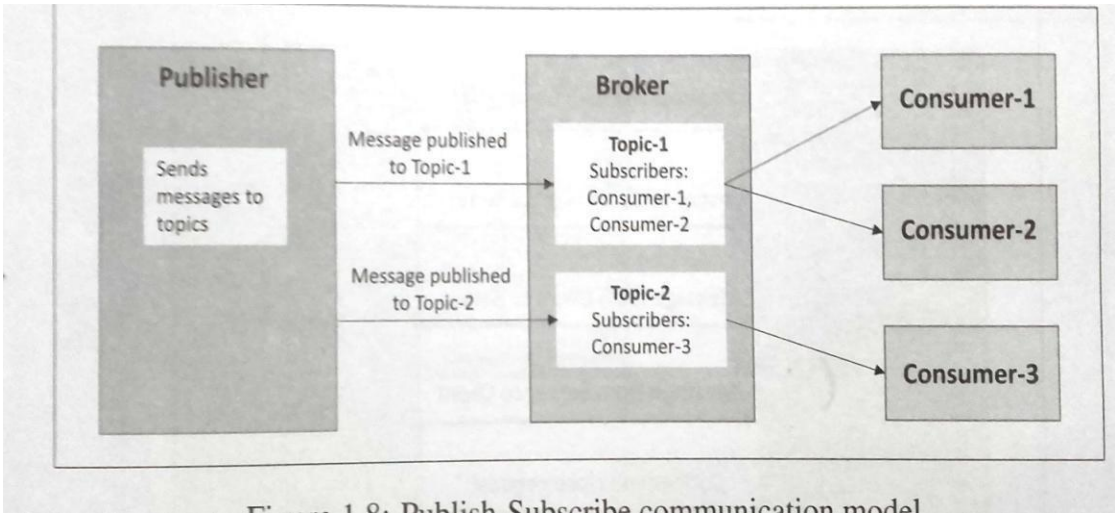
1) Request-Response 2) Publish-Subscibe 3)Push-Pull4) ExclusivePair

1) Request-Response Model:



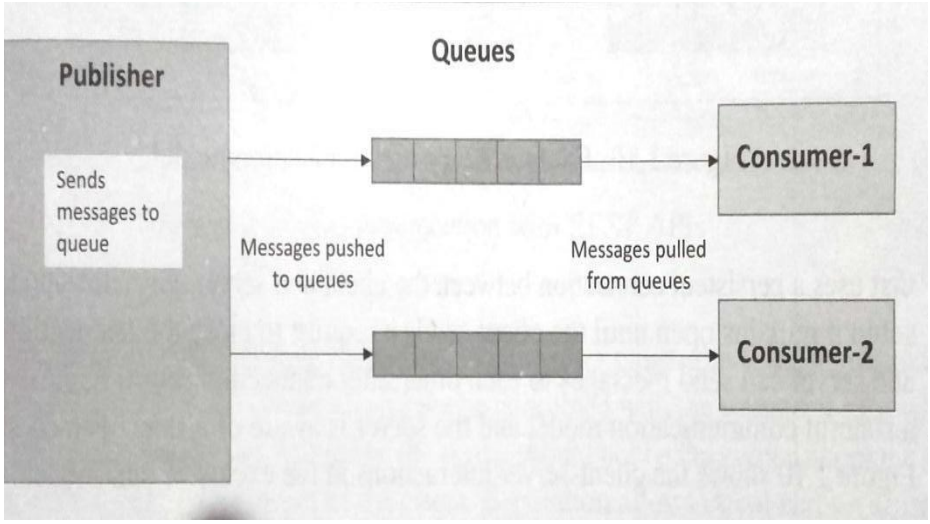
In which the client sends request to the server and the server replies to requests. Is a stateless communication model and each request-response pair is independent of others.

2) **Publish-Subscibe Model:**

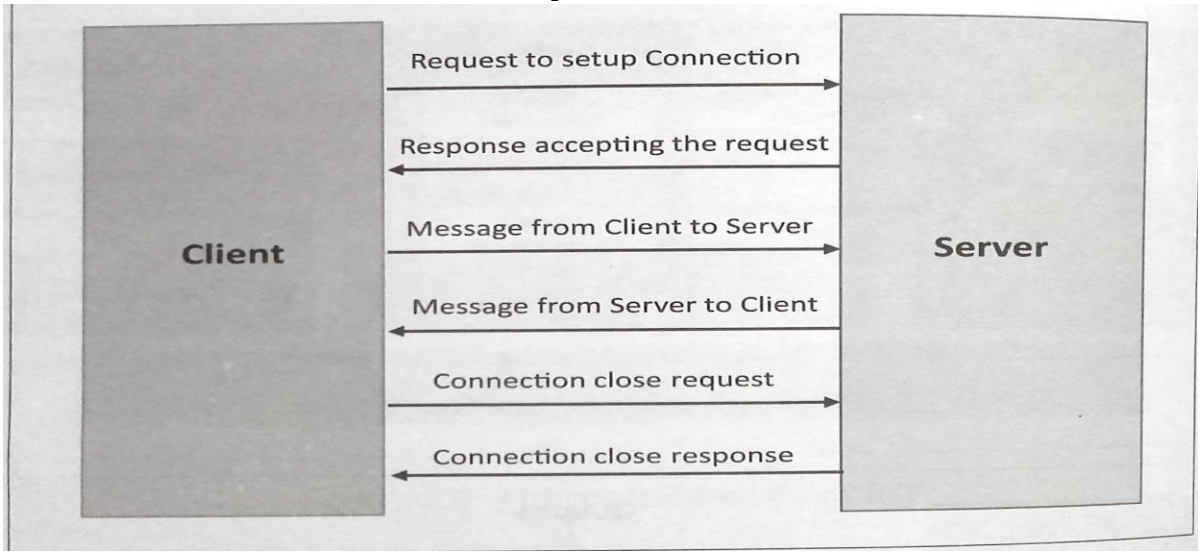


Involves publishers, brokers and consumers. Publishers are source of data. Publishers send data to the topics which are managed by the broker. Publishers are not aware of the consumers. Consumers subscribe to the topics which are managed by the broker. When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.

3) **Push-Pull Model:** in which data producers push data to queues and consumers pull data from the queues. Producers do not need to aware of the consumers. Queues help in decoupling the message between the producers and consumers.



4) **Exclusive Pair:** is bi-directional, fully duplex communication model that uses a persistent connection between the client and server. Once connection is set up it remains open until the client send a request to close the connection. Is a stateful communication model and server is aware of all the open connections.



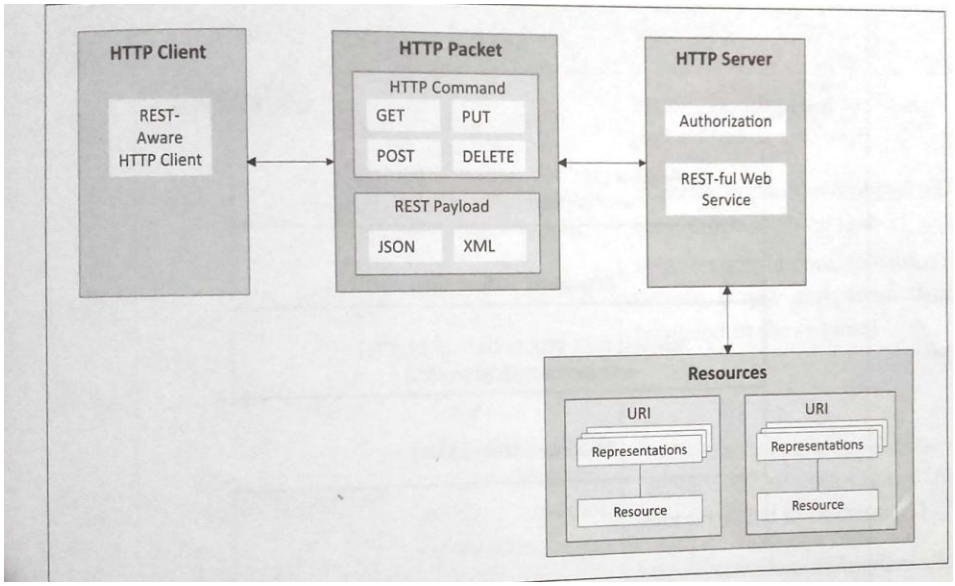
3) IoT Communication APIs:

a) REST based communication APIs(Request-Response Based Model)

b) WebSocket based Communication APIs(Exclusive PairBased Model)

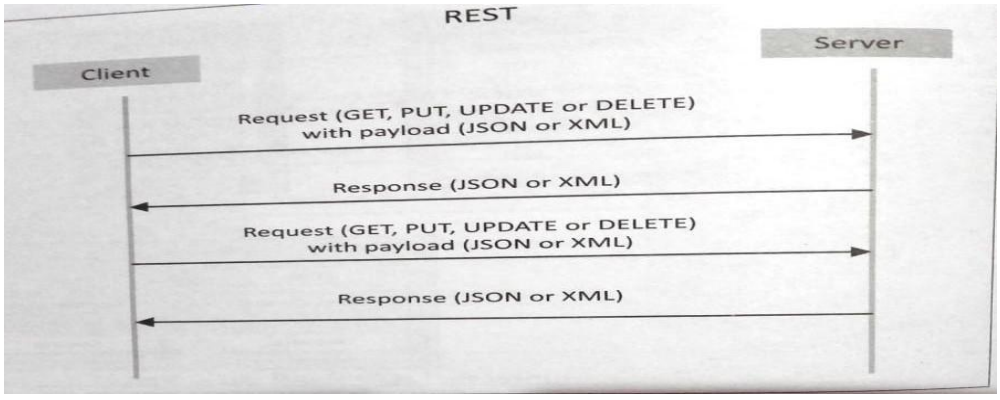
a) REST based communication APIs: Representational State Transfer(REST) is a set of architectural principles by which we can design web services and web APIs that focus on a system‘s resources and have resource states are addressed and transferred.

The REST architectural constraints: Fig. shows communication between client server with REST APIs.



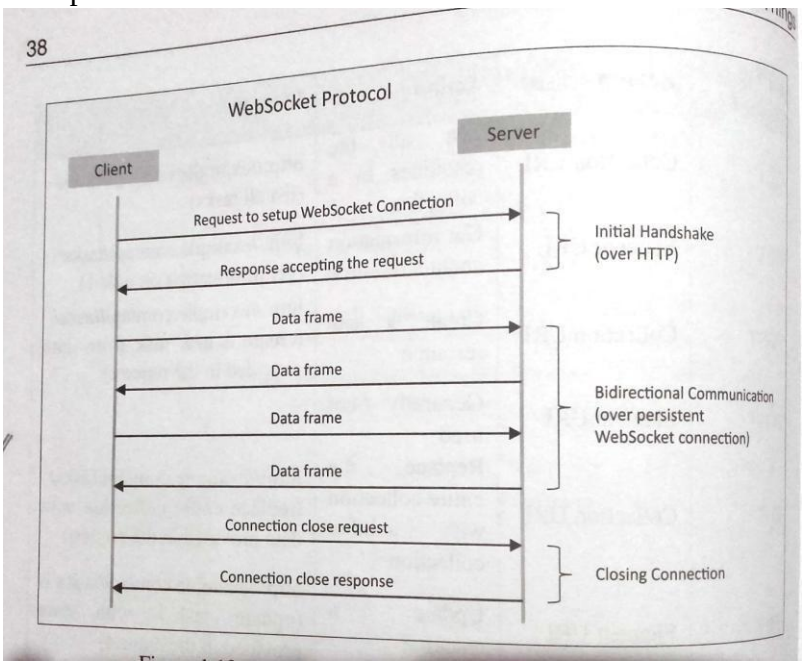
Client-Server: The principle behind client-server constraint is the separation of concerns. Separation allows client and server to be independently developed and updated.
Stateless: Each request from client to server must contain all the info. Necessary to understand the request, and cannot take advantage of any stored context on the server.
Cache-able: Cache constraint requires that the data within a response to a request be implicitly or explicitly labeled as cache-able or non-cacheable. If a response is cache-able, then a client cache is given the right to reuse that response data for later, equivalent requests.
Layered System: constraints the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting.
User Interface: constraint requires that the method of communication between a client and a server must be uniform.
Code on Demand: Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.

Request-Response model used by REST:



RESTful web service is a collection of resources which are represented by URIs. RESTful web API has a base URI(e.g: http://example.com/api/tasks/). The clients and requests to these URIs using the methods defined by the HTTP protocol(e.g: GET, PUT, POST or DELETE). A RESTful web service can support various internet media types.

b) WebSocket Based Communication APIs: WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follow the exclusive pair communication model.



IoT Enabling Technologies

IoT is enabled by several technologies including Wireless Sensor Networks, Cloud Computing, Big Data Analytics, Embedded Systems, Security Protocols and architectures, Communication Protocols, Web Services, Mobile internet and semantic search engines.

1) **Wireless Sensor Network(WSN):** Comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. Zig Bee is one of the most popular wireless technologies used byWSNs.
   WSNs used in IoT systems are described as follows:
   - Weather Monitoring System: in which nodes collect temp, humidity and other data, which is aggregated and analyzed.
   - Indoor air quality monitoring systems: to collect data on the indoor air quality and concentration of various gases.
   - Soil Moisture Monitoring Systems: to monitor soil moisture at variouslocations.
   - Surveillance Systems: use WSNs for collecting surveillance data(motiondata detection).
   - Smart Grids : use WSNs for monitoring grids at variouspoints.

- Structural Health Monitoring Systems: Use WSNs to monitor the health of structures(building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.

2) **Cloud Computing:** Services are offered to users in different forms.
   - Infrastructure-as-a-service(IaaS):provides users the ability to provision computing and storage resources. These resources are provided to the users as a virtual machine instances and virtual storage.
   - Platform-as-a-Service(PaaS): provides users the ability to develop and deploy application in cloud using the development tools, APIs, software libraries and services provided by the cloud service provider.
   - Software-as-a-Service(SaaS): provides the user a complete software application or the user interface to the application itself.

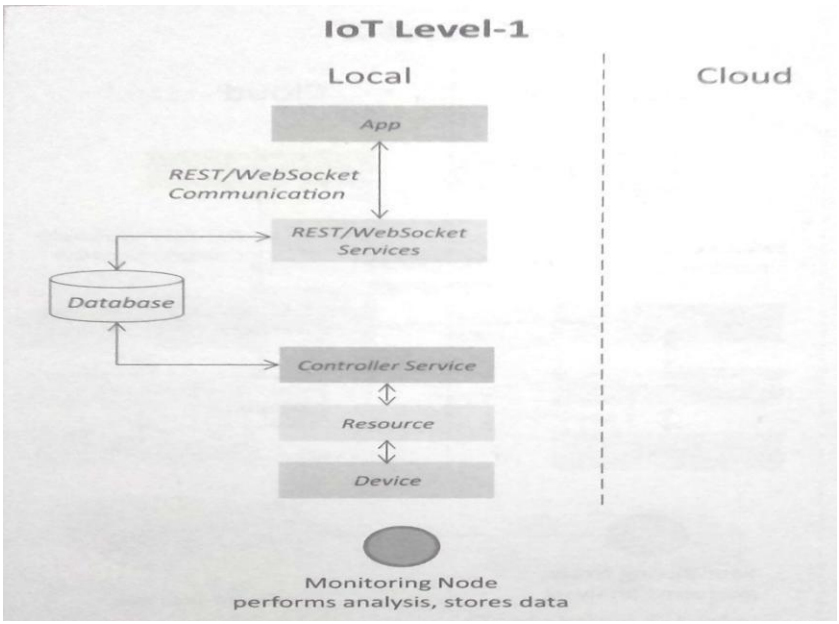
3) **Big Data Analytics:** Some examples of big data generated by IoT are
   - Sensor data generated by IoT systems.
   - Machine sensor data collected from sensors established in industrial and energy systems.
   - Health and fitness data generated IoT devices.
   - Data generated by IoT systems for location and tracking vehicles.
   - Data generated by retail inventory monitoring systems.

4) **Communication Protocols:** form the back-bone of IoT systems and enable network connectivity and coupling to applications.
   - Allow devices to exchange data over network.
   - Define the exchange formats, data encoding addressing schemes for device and routing of packets from source to destination.
   - It includes sequence control, flow control and retransmission of lost packets.

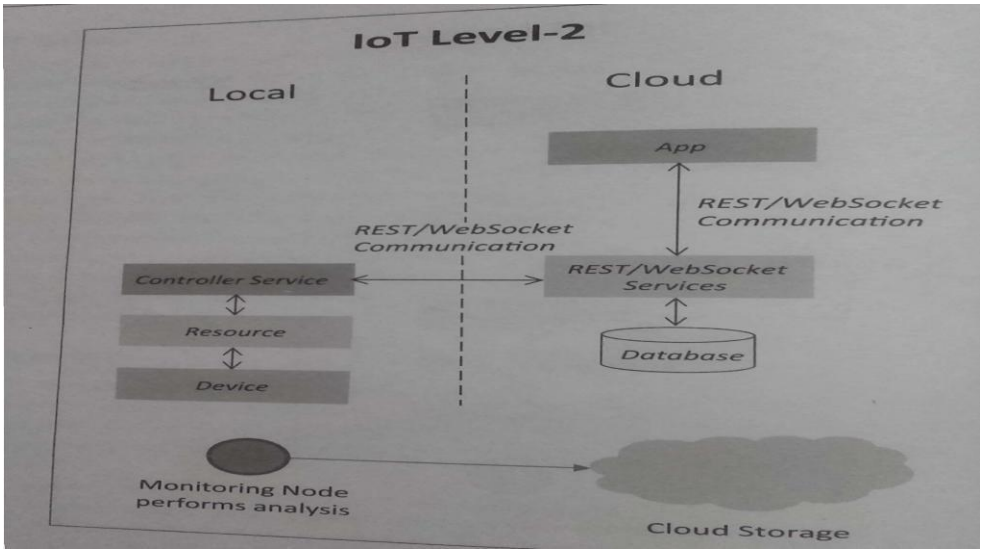
5) **Embedded Systems:** is a computer system that has computer hardware and software embedded to perform specific tasks. Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc.,

IoT Levels and Deployment Templates

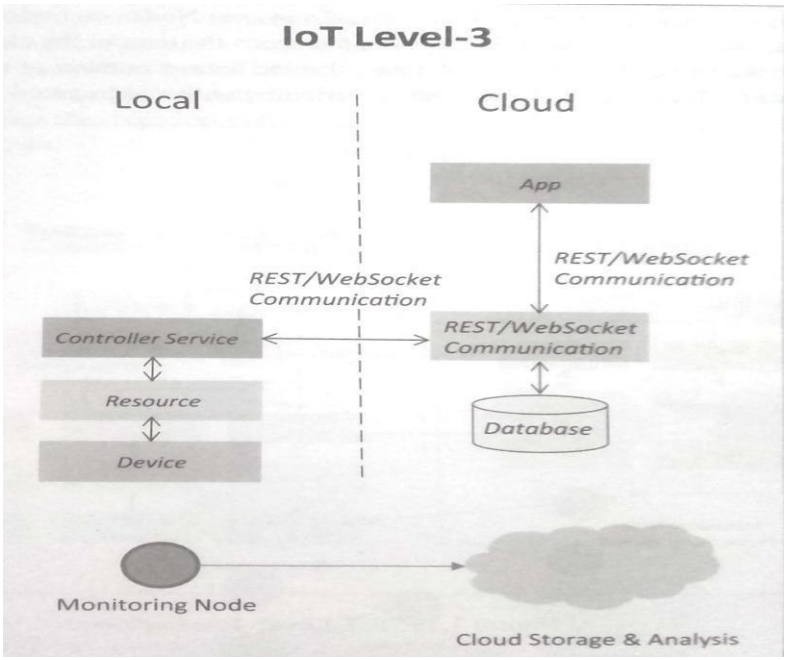
1) **IoT Level1:** System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level1 is Home automation.



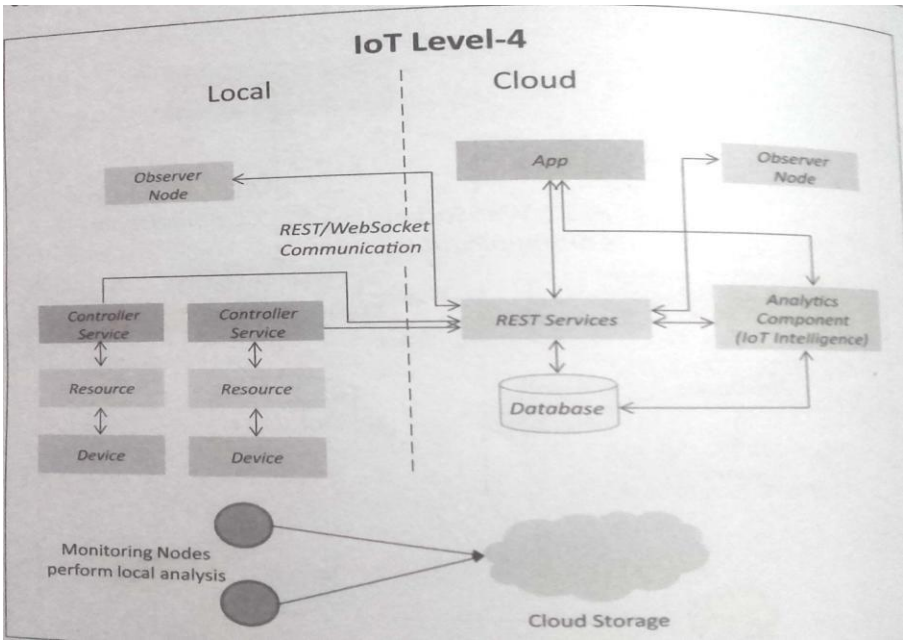
2) **IoT Level2:** has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. An e,g.**,** of Level2 IoT system for Smart Irrigation.



3) **IoT Level3:** system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example of IoT level3 system for tracking package handling.

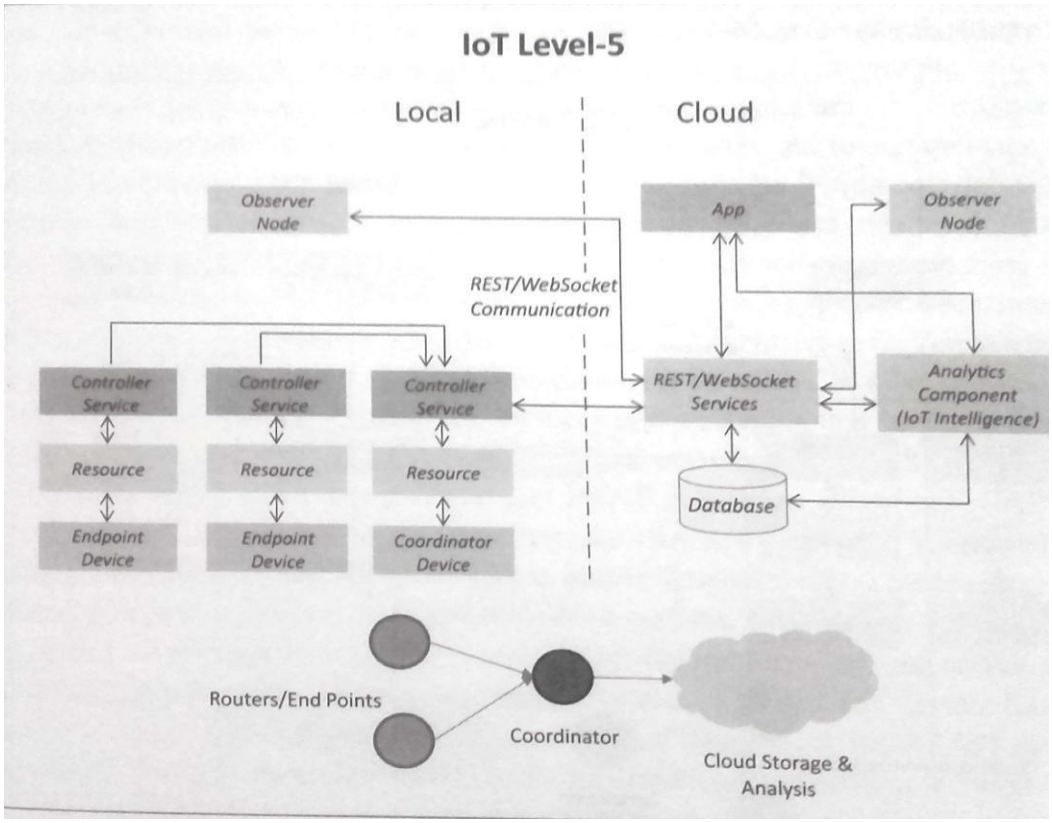


4) **IoT Level4:** System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example of a Level4 IoT system for Noise Monitoring.

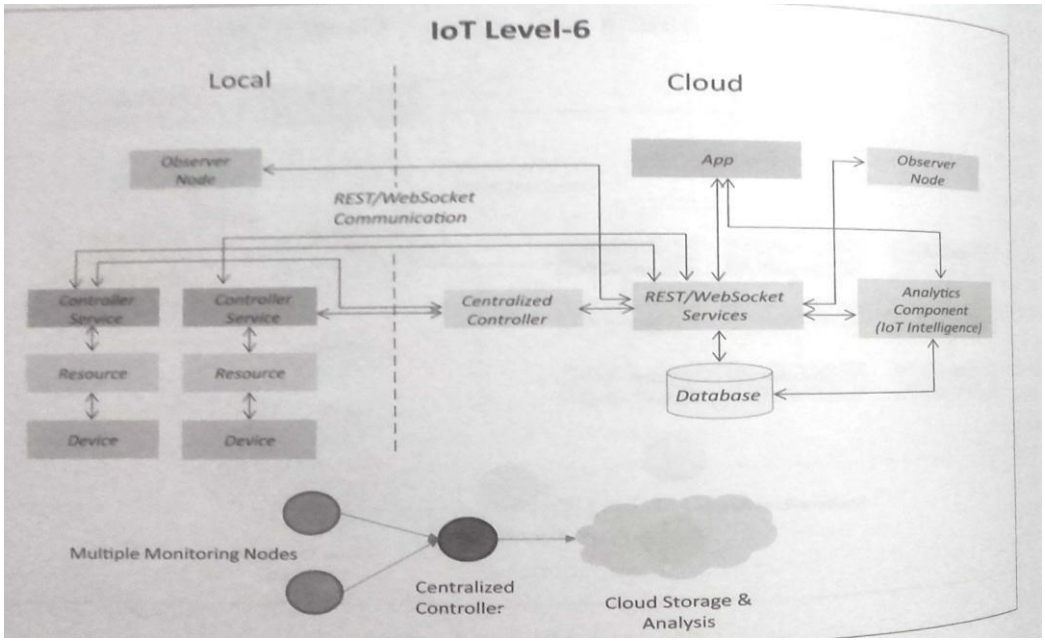


5) **IoT Level5:** System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data from theendnodesandsendstothecloud.Dataisstoredandanalyzedinthecloudand

application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, in which data involved is big and analysis requirements are computationally intensive. An example of Level5 system for Forest Fire Detection.



6) **IoT Level6:** System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud data base. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends control commands to nodes. An example of a Level6 IoT system for Weather Monitoring System.



DOMAIN SPECIFIC IoTs

1) **Home Automation:**
   a) **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed.
   b) **Smart Appliances:** make the management easier and also provide status information to the users remotely.
   c) **Intrusion Detection:** use security cameras and sensors(PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.
   d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPGetc.,

2) **Cities:**
   a) **Smart Parking:** make the search for parking space easier and convenient for drivers. Smart parking are powered by IoT systems that detect the no. of empty parking slots and send information over internet to smart application backends.
   b) **Smart Lighting:** for roads, parks and buildings can help in saving energy.
   c) **Smart Roads:** Equipped with sensors can provide information on driving condition, travel time estimating and alert in case of poor driving conditions, traffic condition and accidents.
   d) **Structural Health Monitoring:** uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.
   e) **Surveillance:** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution.

f) **Emergency Response:** IoT systems for fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructures.

3) Environment:

a) **Weather Monitoring:** Systems collect data from a no. of sensors attached and send the data to cloud based applications and storage back ends. The data collected in cloud can then be analyzed and visualized by cloud based applications.

b) **Air Pollution Monitoring:** System can monitor emission of harmful gases(CO2, CO, NO, NO2 etc.,) by factories and automobiles using gaseous and meteorological sensors. The collected data can be analyzed to make informed decisions on pollutions control approaches.

c) **Noise Pollution Monitoring:** Due to growing urban development, noise levels in cities have increased and even become alarmingly high in some cities. IoT based noise pollution monitoring systems use a no. of noise monitoring systems that are deployed at different places in a city. The data on noise levels from the station is collected on servers or in the cloud. The collected data is then aggregated to generate noise maps.

d) **Forest Fire Detection:** Forest fire can cause damage to natural resources, property and human life. Early detection of forest fire can help in minimizing damage.

e) **River Flood Detection:** River floods can cause damage to natural and human resources and human life. Early warnings of floods can be given by monitoring the water level and flow rate. IoT based river flood monitoring system uses a no. of sensor nodes that monitor the water level and flow rate sensors.

4) Energy:

a) **Smart Grids:** is a data communication network integrated with the electrical grids that collects and analyze data captured in near-real-time about power transmission, distribution and consumption. Smart grid technology provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power. By using IoT based sensing and measurement technologies, the health of equipment and integrity of the grid can be evaluated.

b) **Renewable Energy Systems:** IoT based systems integrated with the transformers at the point of interconnection measure the electrical variables and how much power is fed into the grid. For wind energy systems, closed-loop controls can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputs and provides power support.

c) **Prognostics:** In systems such as power grids, real-time information is collected using specialized electrical sensors called Phasor Measurment Units(PMUs) at the substations. The information received from PMUs must be monitored in real-time for estimating the state of the system and for predicting failures.

5) Retail:

a) **Inventory Management:** IoT systems enable remote monitoring of inventory using data collected by RFIDreaders.

b) **Smart Payments:** Solutions such as contact-less payments powered by technologies such as Near Field Communication(NFC) and Bluetooth.
c) **Smart Vending Machines:** Sensors in a smart vending machines monitors its operations and send the data to cloud which can be used for predictive maintenance.

6) Logistics:

a) **Route generation & scheduling:** IoT based system backed by cloud can provide first response to the route generation queries and can be scaled upto serve a large transportation network.
b) **Fleet Tracking:** Use GPS to track locations of vehicles inreal-time.
c) **Shipment Monitoring:** IoT based shipment monitoring systems use sensors such as temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect foods poilage.
d) **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting data on Vehicle operations(speed, RPMetc.,) and status of various vehicle subsystems.

7) Agriculture:

a) **Smart Irrigation:** to determine moisture amount in soil.
b) **Green House Control:** to improve productivity.

8) Industry:

a) Machine diagnosis and prognosis
b) Indoor Air Quality Monitoring

9) Health and LifeStyle:

a) Health & Fitness Monitoring
b) Wearable Electronics

UNIT-2

Chapter 3

Smart Objects: The "Things" in IoT

Imagine the IoT-enabled connected vehicle and roadway highlighted in Chapter 1, "What Is IoT?" That car has an impressive ecosystem of sensors that provides an immense amount of data that can be intelligently consumed by a variety of systems and services on the car itself as well as shared externally with other vehicles, the connected roadway infrastructure, or even a whole host of other cloud-based diagnostic and consumer services. From behind the steering wheel, almost everything in the car can be checked (sensed) and controlled. The car is filled with sensors of all types (for example, temperature, location [GPS], pressure, velocity) that are meant to provide a wealth of rich and relevant data to, among many other things, improve safety, simplify vehicle maintenance, and enhance the driver experience.

Such sensors are fundamental building blocks of IoT networks. In fact, they are the foundational elements found in smart objects—the "things" in the Internet of Things. Smart objects are any physical objects that contain embedded technology to sense and/or interact with their environment in a meaningful way by being interconnected and enabling communication among themselves or an external agent.

This chapter provides a detailed analysis of smart objects and their architecture. It also provides an understanding of their design limitations and role within IoT networks. Specifically, the following sections are included:

- **Sensors, Actuators, and Smart Objects:** This section defines sensors, actuators, and smart objects and describes how they are the fundamental building blocks of IoT networks.
- **Sensor Networks:** This section covers the design, drivers for adoption, and deployment challenges of sensor networks.

Sensors, Actuators, and Smart Objects

The following sections describe the capabilities, characteristics, and functionality of sensors and actuators. They also detail how the economic and technical conditions are finally right for IoT to flourish. Finally, you will see how to bring these foundational elements together to form smart objects, which are connected to form the sensor and actuator networks that make most IoT use cases possible.

Sensors

A sensor does exactly as its name indicates: It senses. More specifically, a sensor measures some physical quantity and converts that measurement reading into a digital representation. That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans.

Naturally, a parallel can be drawn with humans and the use of their five senses to learn about their surroundings. Human senses do not operate independently in silos. Instead, they complement each other and compute together, empowering the human brain to make intelligent decisions. The brain is the ultimate decision maker, and it often uses several sources of sensory input to validate an event and compensate for "incomplete" information.

Sensors are not limited to human-like sensory data. They can measure anything worth measuring. In fact, they are able to provide an extremely wide spectrum of rich and diverse measurement data with far greater precision than human senses; sensors provide superhuman sensory capabilities. This additional dimension of data makes the physical world an incredibly valuable source of information. Sensors can be readily embedded in any physical objects that are easily connected to the Internet by wired or wireless networks. Because these connected host physical objects with multidimensional sensing capabilities communicate with each other and external systems, they can interpret their environment and make intelligent decisions. Connecting sensing devices in this way has ushered in the world of IoT and a whole new paradigm of business intelligence.

There are myriad different sensors available to measure virtually everything in the physical world. There are a number of ways to group and cluster sensors into different categories, including the following:

- **Active or passive:** Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically require no external power supply (passive).
- **Invasive or non-invasive:** Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).
- **Contact or no-contact:** Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
- **Absolute or relative:** Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).

- **Area of application:** Sensors can be categorized based on the specific industry or vertical where they are being used.
- **How sensors measure:** Sensors can be categorized based on the physical mechanism used to measure sensory input (for example, thermoelectric, electrochemical, piezo-resistive, optic, electric, fluid mechanic, photoelastic).
- **What sensors measure:** Sensors can be categorized based on their applications or what physical variables they measure.

Note that this is by no means an exhaustive list, and there are many other classification and taxonomic schemes for sensors, including those based on material, cost, design, and other factors. The most useful classification scheme for the pragmatic application of sensors in an IoT network, as described in this book, is to simply classify based on what physical phenomenon a sensor is measuring. This type of categorization is shown in Table 3-1.

Table 3-1 *Sensor Types*

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Sensor Types	Description	Examples
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

Source: J. Holdowsky et al., *Inside the Internet of Things: A Primer on the Technologies Building the IoT*, August 21, 2015, http://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-primer-iot-technologies-applications.html.

Sensors come in all shapes and sizes and, as shown in Table 3-1, can measure all types of physical conditions. A fascinating use case to highlight the power of sensors and IoT is in the area of precision agriculture (sometimes referred to as smart farming), which uses a variety of technical advances to improve the efficiency, sustainability, and profitability

of traditional farming practices. This includes the use of GPS and satellite aerial imagery for determining field viability; robots for high-precision planting, harvesting, irrigation, and so on; and real-time analytics and artificial intelligence to predict optimal crop yield, weather impacts, and soil quality.

Among the most significant impacts of precision agriculture are those dealing with sensor measurement of a variety of soil characteristics. These include real-time measurement of soil quality, pH levels, salinity, toxicity levels, moisture levels for irrigation planning, nutrient levels for fertilization planning, and so on. All this detailed sensor data can be analyzed to provide highly valuable and actionable insight to boost productivity and crop yield. Figure 3-1 shows biodegradable, passive microsensors to measure soil and crop and conditions. These sensors, developed at North Dakota State University (NDSU), can be planted directly in the soil and left in the ground to biodegrade without any harm to soil quality.

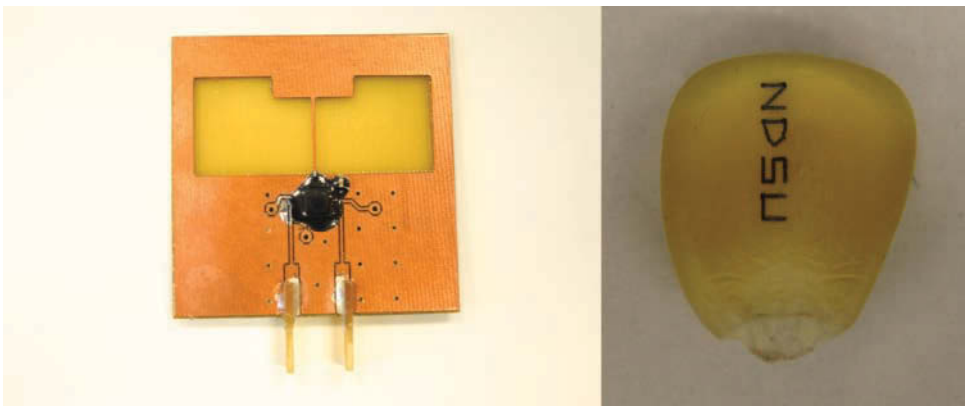


Figure 3-1 *Biodegradable Sensors Developed by NDSU for Smart Farming (Reprinted with permission from NDSU.)*

IoT and, by extension, networked sensors have been repeatedly named among a small number of emerging revolutionary technologies that will change the global economy and shape the future. The staggering proliferation of sensors is the principal driver of this phenomenon. The astounding volume of sensors is in large part due to their smaller size, their form factor, and their decreasing cost. These factors make possible the economic and technical feasibility of having an increased density of sensors in objects of all types. Perhaps the most significant accelerator for sensor deployments is mobile phones. More than a billion smart phones are sold each year, and each one has well over a dozen sensors inside it (see Figure 3-2), and that number continues to grow each year. Imagine the exponential effect of extending sensors to practically every technology, industry, and vertical. For example, there are smart homes with potentially hundreds of sensors, intelligent vehicles with 100+ sensors each, connected cities with thousands upon thousands of connected sensors, and the list goes on and on.

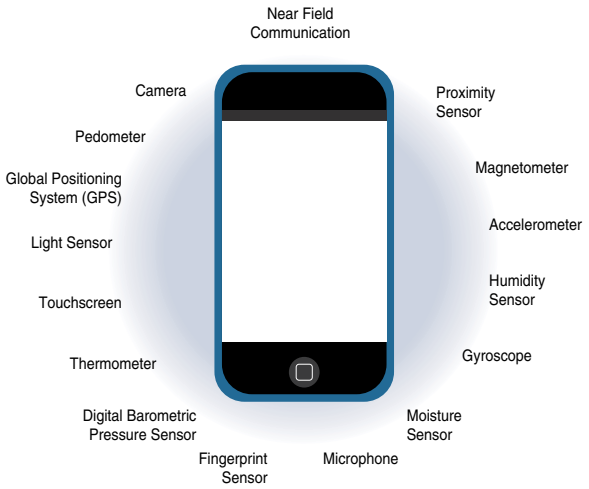


Figure 3-2 *Sensors in a Smart Phone*

It's fascinating to think that that a trillion-sensor economy is around the corner. Figure 3-3 shows the explosive year-over-year increase over the past several years and some bold predictions for sensor numbers in the upcoming years. There is a strong belief in the sensor industry that this number will eclipse a trillion in the next few years. In fact, many large players in the sensor industry have come together to form industry consortia, such as the TSensors Summits (www.tsensorssummit.org), to create a strategy and roadmap for a trillion-sensor economy. The trillion-sensor economy will be of such an unprecedented and unimaginable scale that it will change the world forever. This is the power of IoT.

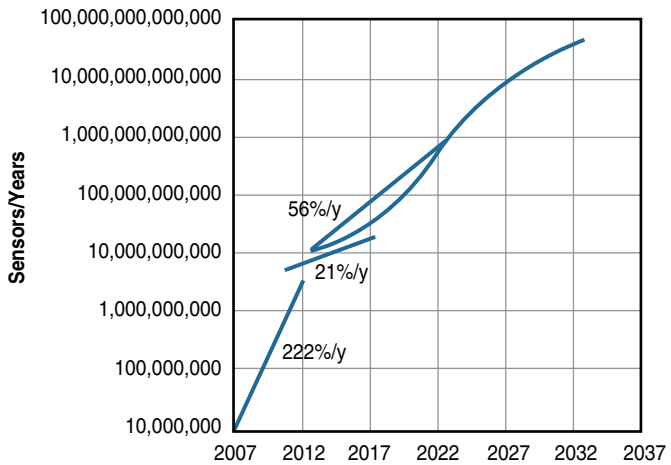


Figure 3-3 *Growth and Predictions in the Number of Sensors*

Actuators

Actuators are natural complements to sensors. Figure 3-4 demonstrates the symmetry and complementary nature of these two types of devices. As discussed in the previous section, sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human). Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.

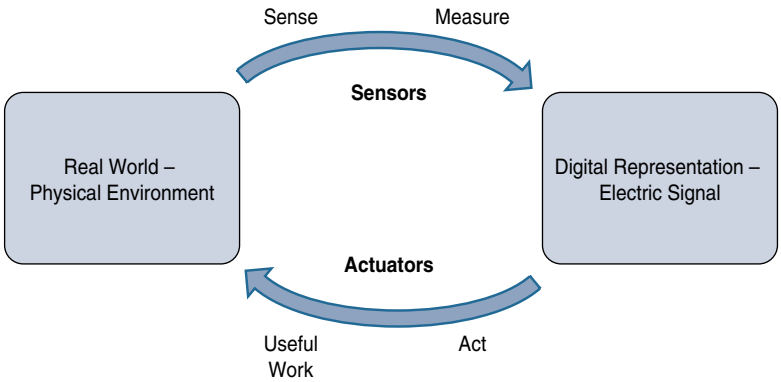


Figure 3-4 *How Sensors and Actuators Interact with the Physical World*

The previous section draws a parallel between sensors and the human senses. This parallel can be extended to include actuators, as shown in Figure 3-5. Humans use their five senses to sense and measure their environment. The sensory organs convert this sensory information into electrical impulses that the nervous system sends to the brain for processing. Likewise, IoT sensors are devices that sense and measure the physical world and (typically) signal their measurements as electric signals sent to some type of microprocessor or microcontroller for additional processing. The human brain signals motor function and movement, and the nervous system carries that information to the appropriate part of the muscular system. Correspondingly, a processor can send an electric signal to an actuator that translates the signal into some type of movement (linear, rotational, and so on) or useful work that changes or has a measurable impact on the physical world. This interaction between sensors, actuators, and processors and the similar functionality in biological systems is the basis for various technical fields, including robotics and biometrics.

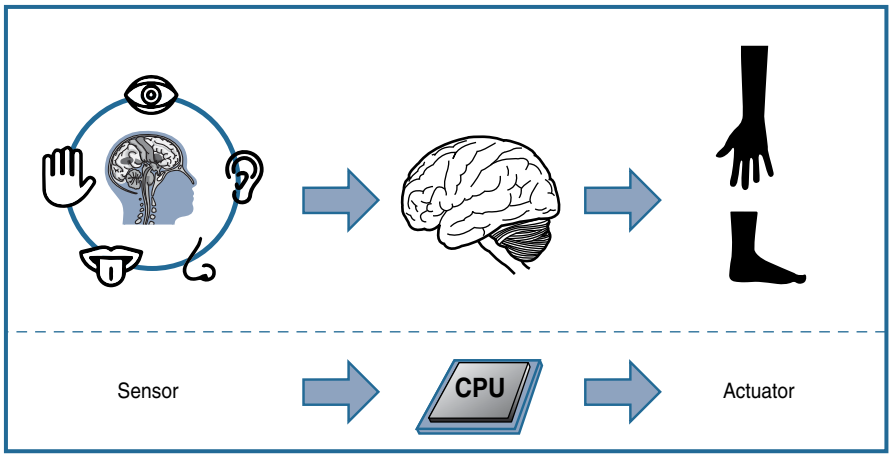


Figure 3-5 *Comparison of Sensor and Actuator Functionality with Humans*

Much like sensors, actuators also vary greatly in function, size, design, and so on. Some common ways that they can be classified include the following:

- **Type of motion:** Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).
- **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power)
- **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.
- **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.
- **Type of energy:** Actuators can be classified based on their energy type.

Categorizing actuators is quite complex, given their variety, so this is by no means an exhaustive list of classification schemes. The most commonly used classification is based on energy type. Table 3-2 shows actuators classified by energy type and some examples for each type. Again, this is not a complete list, but it does provide a reasonably comprehensive overview that highlights the diversity of function and design of actuators.

Table 3-2 *Actuator Classification by Energy Type*

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor

Type	Examples
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

Whereas sensors provide the information, actuators provide the action. The most interesting use cases for IoT are those where sensors and actuators work together in an intelligent, strategic, and complementary fashion. This powerful combination can be used to solve everyday problems by simply elevating the data that sensors provide to actionable insight that can be acted on by work-producing actuators.

We can build on the precision agriculture example from the previous section to demonstrate how actuators can complement and enhance a sensor-only solution. For example, the smart sensors used to evaluate soil quality (by measuring a variety of soil, temperature, and plant characteristics) can be connected with electrically or pneumatically controlled valve actuators that control water, pesticides, fertilizers, herbicides, and so on. Intelligently triggering a high-precision actuator based on well-defined sensor readings of temperature, pH, soil/air humidity, nutrient levels, and so on to deliver a highly optimized and custom environment-specific solution is truly smart farming.

Micro-Electro-Mechanical Systems (MEMS)

One of the most interesting advances in sensor and actuator technologies is in how they are packaged and deployed. Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale. One of the keys to this technology is a microfabrication technique that is similar to what is used for microelectronic integrated circuits. This approach allows mass production at very low costs. The combination of tiny size, low cost, and the ability to mass produce makes MEMS an attractive option for a huge number of IoT applications.

MEMS devices have already been widely used in a variety of different applications and can be found in very familiar everyday devices. For example, inkjet printers use micro-pump MEMS. Smart phones also use MEMS technologies for things like accelerometers and gyroscopes. In fact, automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers.

Figure 3-6 shows a torsional ratcheting actuator (TRA) that was developed by Sandia National Laboratory as a low-voltage alternative to a micro-engine.

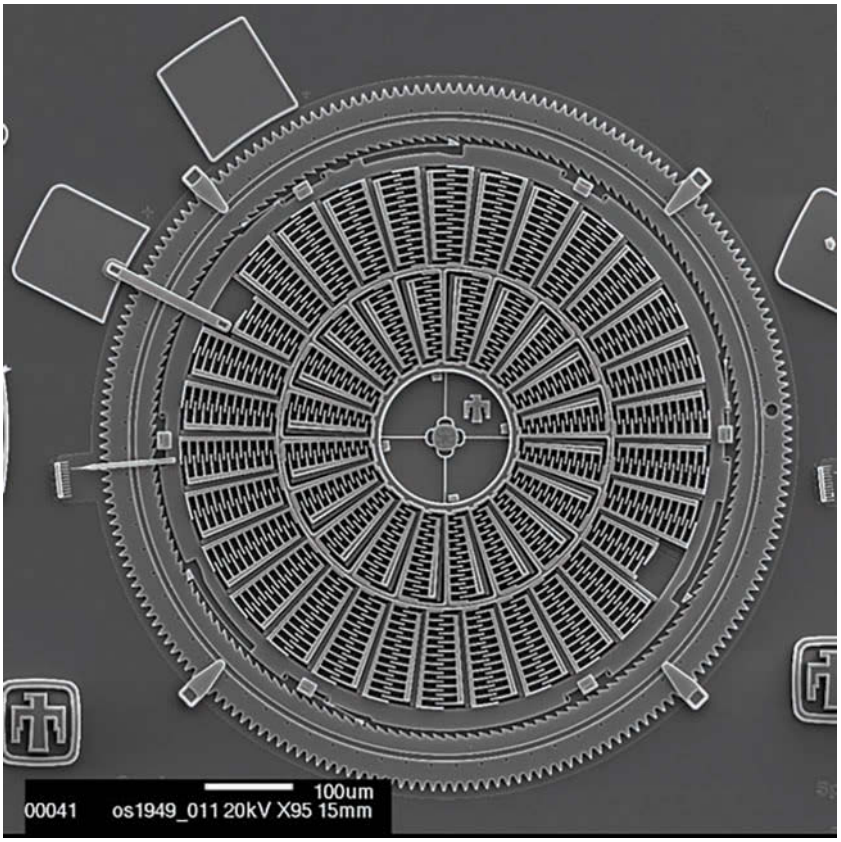


Figure 3-6 *Torsional Ratcheting Actuator (TRA) MEMS (Courtesy Sandia National Laboratories, SUMMiT™ Technologies, www.sandia.gov/mstc.)*

As Figure 3-6 shows, this MEMS is only a few hundred micrometers across; a scanning electron microscope is needed to show the level of detail visible in the figure. Micro-scale sensors and actuators are immensely embeddable in everyday objects, which is a defining characteristic of IoT. For this reason, it is expected that IoT will trigger significant advances in MEMS technology, and manufacturing and will make them pervasive across all industries and verticals as they become broadly commercialized.

Smart Objects

Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way. It can't be stressed enough that the real power of smart objects in IoT comes from being networked together rather than being isolated as standalone objects. This ability to communicate over a network has a multiplicative effect and allows for very sophisticated correlation and interaction between disparate smart objects. For instance, recall the smart farming sensors described

previously. If a sensor is a standalone device that simply measures the humidity of the soil, it is interesting and useful, but it isn't revolutionary. If that same sensor is connected as part of an intelligent network that is able to coordinate intelligently with actuators to trigger irrigation systems as needed based on those sensor readings, we have something far more powerful. Extending that even further, imagine that the coordinated sensor/actuator set is intelligently interconnected with other sensor/actuator sets to further coordinate fertilization, pest control, and so on—and even communicate with an intelligent backend to calculate crop yield potential. This now starts to look like a complete system that begins to unlock the power of IoT and provides the intelligent automation we have come to expect from such a revolutionary technology.

Smart Objects: A Definition

Historically, the definition of a smart object has been a bit nebulous because of the different interpretations of the term by varying sources. To add to the overall confusion, the term *smart object*, despite some semantic differences, is often used interchangeably with terms such as *smart sensor*, *smart device*, *IoT device*, *intelligent device*, *thing*, *smart thing*, *intelligent node*, *intelligent thing*, *ubiquitous thing*, and *intelligent product*. In order to clarify some of this confusion, we provide here the definition of *smart object* as we use it in this book. A *smart object*, as described throughout this book, is a device that has, at a minimum, the following four defining characteristics (see Figure 3-7):

- **Processing unit:** A smart object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensor(s), coordinating control signals to any actuators, and controlling a variety of functions on the smart object, including the communication and power systems. The specific type of processing unit that is used can vary greatly, depending on the specific processing needs of different applications. The most common is a microcontroller because of its small form factor, flexibility, programming simplicity, ubiquity, low power consumption, and low cost.
- **Sensor(s) and/or actuator(s):** A smart object is capable of interacting with the physical world through sensors and actuators. As described in the previous sections, a sensor learns and measures its environment, whereas an actuator is able to produce some change in the physical world. A smart object does not need to contain both sensors and actuators. In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.
- **Communication device:** The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network). Communication devices for smart objects can be either wired or wireless. Overwhelmingly, in IoT networks smart objects are wirelessly interconnected for a number of reasons, including cost, limited infrastructure availability, and ease of deployment. There are myriad different communication protocols for smart objects. In fact, much of this book is dedicated to how smart objects communicate within an IoT network, especially Chapter 4, "Connecting Smart Objects," Chapter 5,

"IP as the IoT Network Layer," and Chapter 6, "Application Protocols for IoT." Thus, this chapter provides only a high-level overview and refers to those other chapters for a more detailed treatment of the subject matter.

- **Power source:** Smart objects have components that need to be powered. Interestingly, the most significant power consumption usually comes from the communication unit of a smart object. As with the other three smart object building blocks, the power requirements also vary greatly from application to application. Typically, smart objects are limited in power, are deployed for a very long time, and are not easily accessible. This combination, especially when the smart object relies on battery power, implies that power efficiency, judicious power management, sleep modes, ultra-low power consumption hardware, and so on are critical design elements. For long-term deployments where smart objects are, for all practical purposes, inaccessible, power is commonly obtained from scavenger sources (solar, piezoelectric, and so on) or is obtained in a hybridized manner, also tapping into infrastructure power.

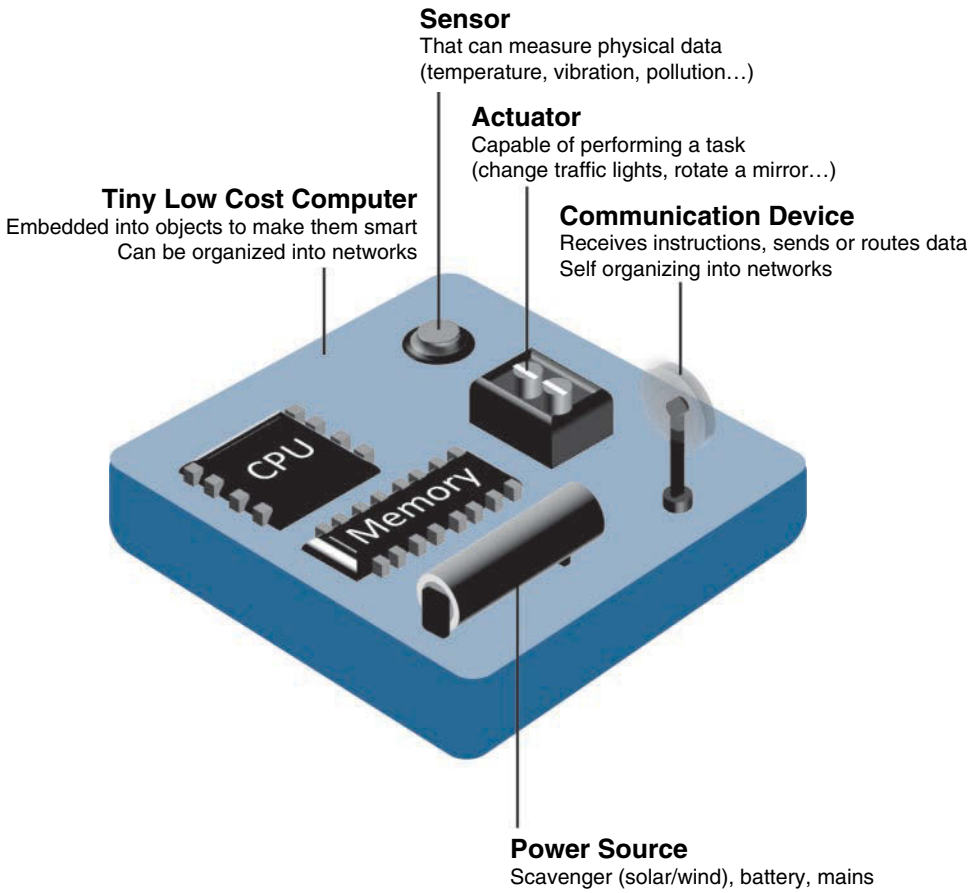


Figure 3-7 *Characteristics of a Smart Object*

Trends in Smart Objects

As this definition reveals, it is perhaps variability that is the key characteristic of smart objects. They vary wildly in function, technical requirements, form factor, deployment conditions, and so on. Nevertheless, there are certain important macro trends that we can infer from recent and planned future smart object deployments. Of course, these do not apply to all smart objects because there will always be application-dependent variability, but these are broad generalizations and trends impacting IoT:

- **Size is decreasing:** As discussed earlier, in reference to MEMS, there is a clear trend of ever-decreasing size. Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.
- **Power consumption is decreasing:** The different hardware components of a smart object continually consume less power. This is especially true for sensors, many of which are completely passive. Some battery-powered sensors last 10 or more years without battery replacement.
- **Processing power is increasing:** Processors are continually getting more powerful and smaller. This is a key advancement for smart objects, as they become increasingly complex and connected.
- **Communication capabilities are improving:** It's no big surprise that wireless speeds are continually increasing, but they are also increasing in range. IoT is driving the development of more and more specialized communication protocols covering a greater diversity of use cases and environments.
- **Communication is being increasingly standardized:** There is a strong push in the industry to develop open standards for IoT communication protocols. In addition, there are more and more open source efforts to advance IoT.

These trends in smart objects begin to paint a picture of increasingly sophisticated devices that are able to perform increasingly complex tasks with greater efficiency. A key enabler of this paradigm is improved communication between interconnected smart objects within a system and between that system and external entities (for example, edge compute, cloud). The power of IoT is truly unlocked when smart objects are networked together in sensor/actuator networks.

Sensor Networks

A sensor/actuator network (SANET), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment. The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner. Effective and well-coordinated communication and cooperation is a prominent challenge, primarily because the sensors and actuators in SANETs are diverse, heterogeneous, and resource-constrained.

SANETs offer highly coordinated sensing and actuation capabilities. Smart homes are a type of SANET that display this coordination between distributed sensors and actuators.

For example, smart homes can have temperature sensors that are strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators. When a sensor detects a specified temperature, this can trigger an actuator to take action and heat or cool the home as needed.

While such networks can theoretically be connected in a wired or wireless fashion, the fact that SANETs are typically found in the "real world" means that they need an extreme level of deployment flexibility. For example, smart home temperature sensors need to be expertly located in strategic locations throughout the home, including at HVAC entry and exit points.

The following are some advantages and disadvantages that a wireless-based solution offers:

- Advantages:
  - Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
  - Simpler scaling to a large number of nodes
  - Lower implementation costs
  - Easier long-term maintenance
  - Effortless introduction of new sensor/actuator nodes
  - Better equipped to handle dynamic/rapid topology changes
- Disadvantages:
  - Potentially less secure (for example, hijacked access points)
  - Typically lower transmission speeds
  - Greater level of impact/influence by environment

Not only does wireless allow much greater flexibility, but it is also an increasingly inexpensive and reliable technology across a very wide spectrum of conditions—even extremely harsh ones. These characteristics are the key reason that wireless SANETs are the ubiquitous networking technology for IoT.

Note From a terminology perspective, wireless SANETs are typically referred to as wireless sensor and actuator networks (WSANs). Because many IoT deployments are overwhelmingly sensors, WSANs are also often interchangeably referred to as wireless sensor networks (WSNs). In this book, we commonly refer to WSANs as WSNs, with the understanding that actuators are often part of the wireless network.

Wireless Sensor Networks (WSNs)

Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as *motes*. The fact that there is no infrastructure to consider with

WSNs is surely a powerful advantage for flexible deployments, but there are a variety of design constraints to consider with these wirelessly connected smart objects. Figure 3-8 illustrates some of these assumptions and constraints usually involved in WSNs.

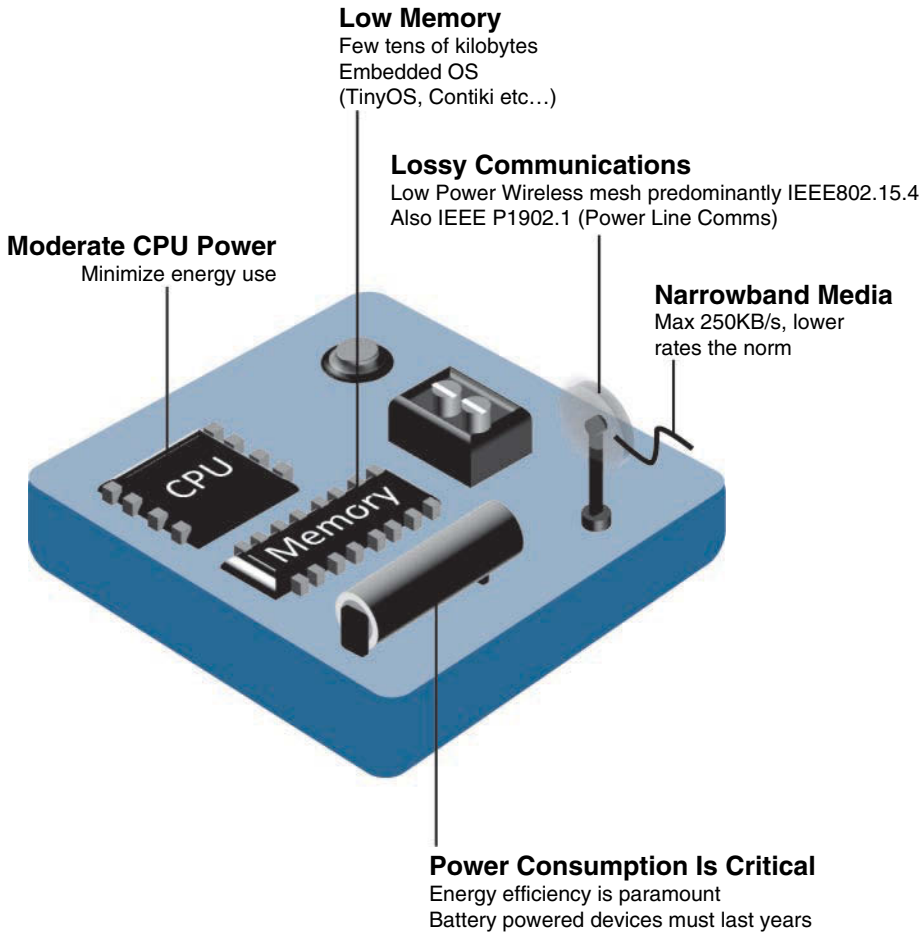


Figure 3-8 *Design Constraints for Wireless Smart Objects*

The following are some of the most significant limitations of the smart objects in WSNs:

- Limited processing power
- Limited memory
- Lossy communication
- Limited transmission speeds
- Limited power

These limitations greatly influence how WSNs are designed, deployed, and utilized. The fact that individual sensor nodes are typically so limited is a reason that they are often deployed in very large numbers. As the cost of sensor nodes continues to decline, the ability to deploy highly redundant sensors becomes increasingly feasible. Because many sensors are very inexpensive and correspondingly inaccurate, the ability to deploy smart objects redundantly allows for increased accuracy.

Note Smart objects with limited processing, memory, power, and so on are often referred to as *constrained nodes*. Constrained nodes are discussed in more detail in Chapter 5.

Such large numbers of sensors permit the introduction of hierarchies of smart objects. Such a hierarchy provides, among other organizational advantages, the ability to aggregate similar sensor readings from sensor nodes that are in close proximity to each other. Figure 3-9 shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.

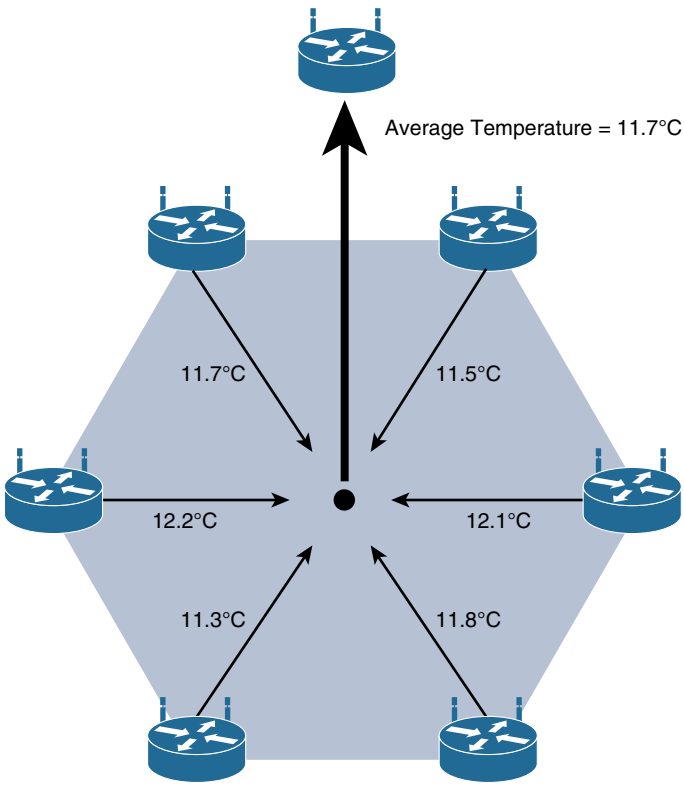


Figure 3-9 *Data Aggregation in Wireless Sensor Networks*

These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSNs with very large numbers of deployed smart objects. This data aggregation at the network edges is where fog and mist computing, discussed in Chapter 2, "IoT Network Architecture and Design," are critical IoT architectural elements needed to deliver the scale and performance required by so many IoT use cases. While there are certain instances in which sensors continuously stream their measurement data, this is typically not the case. Wirelessly connected smart objects generally have one of the following two communication patterns:

- **Event-driven:** Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.
- **Periodic:** Transmission of sensory information occurs only at periodic intervals.

The decision of which of these communication schemes is used depends greatly on the specific application. For example, in some medical use cases, sensors periodically send postoperative vitals, such as temperature or blood pressure readings. In other medical use cases, the same blood pressure or temperature readings are triggered to be sent only when certain critically low or high readings are measured.

As WSNs grow to very large numbers of smart objects, there is a trend toward ever-increasing levels of autonomy. For example, manual configuration of potentially thousands of smart objects is impractical and unwieldy, so smart objects in a WSN are typically self-configuring or automated by an IoT management platform in the background. Likewise, additional levels of autonomous functions are required to establish cohesive communication among the multitudinous nodes of large-scale WSNs that are often ad hoc deployments with no regard for uniform node distribution and/or density. For example, there is an increasing trend toward "smart dust" applications, in which very small sensor nodes (that is, MEMS) are scattered over a geographic area to detect vibrations, temperature, humidity, and so on. This technology has practically limitless capabilities, such as military (for example, detecting enemy troop movement), environmental (for example, detecting earthquakes or forest fires), and industrial (for example, detecting manufacturing anomalies, asset tracking). Some level of self-organization is required for networking the scads of wireless smart objects such that these nodes autonomously come together to form a true network with a common purpose. This capability to self-organize is able to adapt and evolve the logical topology of a WSN to optimize communication (among nodes as well as to centralized wireless controllers), simplify the introduction of new smart objects, and improve reliability and access to services.

Additional advantages of being able to deploy large numbers of wireless low-cost smart objects are the inherent ability to provide fault tolerance, reliability, and the capability to extend the life of a WSN, especially in scenarios where the smart objects have limited battery life. Autonomous techniques, such as self-healing, self-protection, and self-optimization, are often employed to perform these functions on behalf of an overall WSN system. IoT applications are often mission critical, and in large-scale WSNs, the overall system can't fail if the environment suddenly changes, wireless communication is temporarily lost, or a limited number of nodes run out of battery power or function improperly.

Communication Protocols for Wireless Sensor Networks

There are literally thousands of different types of sensors and actuators. To further complicate matters, WSNs are becoming increasingly heterogeneous, with more sophisticated interactions. This heterogeneity is manifested in a variety of ways. For instance, WSNs are seeing transitions from homogenous wireless networks made up of mostly a single type of sensor to networks made up of multiple types of sensors that can even be a hybridized mix of many cheap sensors with a few expensive ones used for very specific high-precision functions. WSNs are also evolving from single-purpose networks to more flexible multipurpose networks that can use specific sensor types for multiple different applications at any given time. Imagine a WSN that has multiple types of sensors, and one of those types is a temperature sensor that can be flexibly used concurrently for environmental applications, weather applications, and smart farming applications.

Coordinated communication with sophisticated interactions by constrained devices within such a heterogeneous environment is quite a challenge. The protocols governing the communication for WSNs must deal with the inherent defining characteristics of WSNs and the constrained devices within them. For instance, any communication protocol must be able to scale to a large number of nodes. Likewise, when selecting a communication protocol, you must carefully take into account the requirements of the specific application and consider any trade-offs the communication protocol offers between power consumption, maximum transmission speed, range, tolerance for packet loss, topology optimization, security, and so on. The fact that WSNs are often deployed outdoors in harsh and unpredictable environments adds yet another variable to consider because obviously not all communication protocols are designed to be equally rugged. In addition to the aforementioned technical capabilities, they must also enable, as needed, the overlay of autonomous techniques (for example, self-organization, self-healing, self-configuration) mentioned in the previous section.

Wireless sensor networks interact with their environment. Sensors often produce large amounts of sensing and measurement data that needs to be processed. This data can be processed locally by the nodes of a WSN or across zero or more hierarchical levels in IoT networks. (These hierarchical levels are discussed in detail in Chapter 2.) Communication protocols need to facilitate routing and message handling for this data flow between sensor nodes as well as from sensor nodes to optional gateways, edge compute, or centralized cloud compute. IoT communication protocols for WSNs thus straddle the entire protocol stack. Ultimately, they are used to provide a platform for a variety of IoT smart services.

As with any other networking application, in order to interoperate in multivendor environments, these communication protocols must be standardized. This is a critical dependency for IoT and one of the most significant success factors. IoT is one of those rare technologies that impacts all verticals and industries, which means standardization of communication protocols is a complicated task, requiring protocol definition across multiple layers of the stack, as well as a great deal of coordination across multiple standards development organizations.

Recently there have been focused efforts to standardize communication protocols for IoT, but, as with the adoption of any significant technology movement, there has been some market fragmentation. While there isn't a single protocol solution, there is beginning to be some clear market convergence around several key communication protocols. We do not spend time here discussing these specific protocols and their detailed operation because large chunks of this book are specifically dedicated to such discussion, including Chapters 4, 5, and 6.

Summary

Wireless sensor and actuator networks are a unique computing platform that can be highly distributed and deployed in unique environments where traditional computing platforms are not typically found. This offers unique advantages and opportunities to interact with and influence those environments. This is the basis of IoT, and it opens up a world of possibility, embedding sensors and/or actuators in everyday objects and networking them to enable sophisticated and well-coordinated automations that improves and simplifies our lives.

This chapter introduces the "things" that are the building blocks of IoT. It includes descriptions and practical examples of sensors and how they are able to measure their environment. It provides the same sort of discussion for actuators, which use environmental sensing information in a complementary way to act on their surroundings. This chapter also highlights recent manufacturing trends (such as MEMS) toward making sensors and actuators ever smaller and more embeddable in everyday objects. This chapter also covers smart objects, which are typically highly constrained devices with sensor(s) and/or actuator(s) along with very limited power, transmission, and compute capabilities.

As discussed in this chapter, we unlock the power of IoT by networking smart objects. Sensor and actuator networks (SANETs) are discussed, with particular attention and detail given to the overwhelmingly ubiquitous use case of wireless sensor networks (WSNs). The last topic discussed in this chapter is communication protocols for WSANs, which sets you up for the next chapter, on connecting smart objects.

This page intentionally left blank

Chapter 4

Connecting Smart Objects

IoT devices and sensors must be connected to the network for their data to be utilized. In addition to the wide range of sensors, actuators, and smart objects that make up IoT, there are also a number of different protocols used to connect them. This chapter takes a look at the characteristics and communications criteria that are important for the **technologies** that smart objects employ for their connectivity, along with a deeper dive into some of the major technologies being deployed today.

Two main sections divide this chapter. The first main section, "Communications Criteria," describes the characteristics and attributes you should consider when selecting and dealing with connecting smart objects. The various technologies used for connecting sensors can differ greatly depending on the criteria used to analyze them. The following subsections look closely at these criteria:

- **Range:** This section examines the importance of signal propagation and distance.
- **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies.
- **Power Consumption:** This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.
- **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.
- **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.
- **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.

The second main section of this chapter, "IoT Access Technologies," provides an in-depth look at some of the technologies that are considered when connecting smart objects. Currently, the number of technologies connecting smart objects is quite extensive, but

you should expect consolidation, with certain protocols eventually winning out over others in the various IoT market segments. This section intentionally limits the discussion of technologies for connecting sensors to the ones that seem to be most promising going forward in the IoT marketplace. Other technologies are mentioned in context when applicable. The following subsections cover technologies for connecting smart objects:

- **IEEE 802.15.4:** This section highlights IEEE 802.15.4, an older but foundational wireless protocol for connecting smart objects.
- **IEEE 802.15.4g and IEEE 802.15.4e:** This section discusses improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
- **IEEE 1901.2a:** This section discusses IEEE 1901.2a, which is a technology for connecting smart objects over power lines.
- **IEEE 802.11ah:** This section discusses IEEE 802.11ah, a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
- **LoRaWAN:** This section discusses LoRaWAN, a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
- **NB-IoT and Other LTE Variations:** This section discusses NB-IoT and other LTE variations, which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

This chapter covers quite a few fundamental IoT technologies and is critical for truly understanding how smart objects handle data transport to and from the network. We encourage you to pay special attention to the protocols and technologies discussed here because they are applied and referenced in many of the other chapters of this book.

Communications Criteria

In the world of connecting "things," a large number of wired and wireless access technologies are available or under development. Before reviewing some of these access technologies, it is important to talk about the criteria to use in evaluating them for various use cases and system solutions.

Wireless communication is prevalent in the world of smart object connectivity, mainly because it eases deployment and allows smart objects to be mobile, changing location without losing connectivity. The following sections take this into account as they discuss various criteria. In addition, wired connectivity considerations are mentioned when applicable.

Range

How far does the signal need to be propagated? That is, what will be the area of coverage for a selected wireless technology? Should indoor versus outdoor deployments be differentiated? Very often, these are the first questions asked when discussing wired

and wireless access technologies. The simplest approach to answering these types of questions is to categorize these technologies as shown in Figure 4-1, breaking them down into the following ranges:

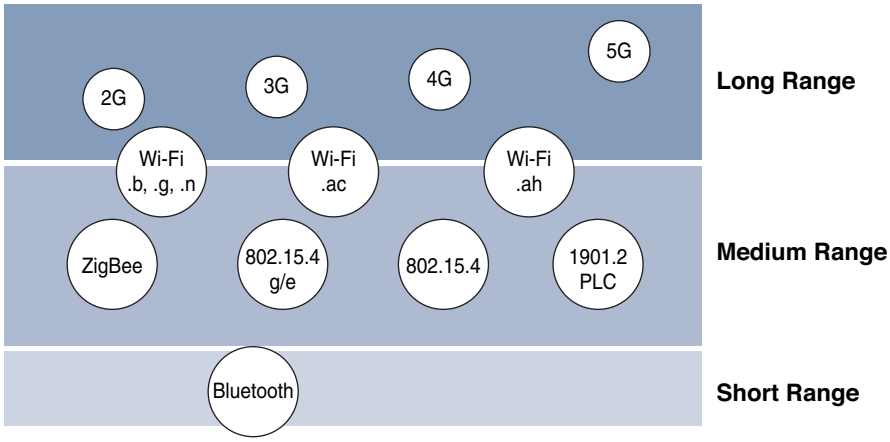


Figure 4-1 *Wireless Access Landscape*

Note Figure 4-1 focuses on the IoT technologies discussed in this chapter. To avoid adding too much confusion by talking about all of the multitude of IoT technologies in the market today, this chapter discusses only the ones that appear to have the strongest foothold.

- **Short range:** The classical wired example is a serial cable. Wireless short-range technologies are often considered as an alternative to a serial cable, supporting tens of meters of maximum distance between two devices. Examples of short-range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC). These short-range communication methods are found in only a minority of IoT installations. In some cases, they are not mature enough for production deployment. For more information on these IEEE examples, see http://standards.ieee.org/about/get/802/802.15.html.
- **Medium range:** This range is the main category of IoT access technologies. In the range of tens to hundreds of meters, many specifications and implementations are available. The maximum distance is generally less than 1 mile between two devices, although RF technologies do not have real maximum distances defined, as long as the radio signal is transmitted and received in the scope of the applicable specification. Examples of medium-range wireless technologies include IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN. Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC) may also be classified as medium range, depending on their physical media

characteristics. (All the medium-range protocols just mentioned are covered in more detail later in this chapter.)

- **Long range:** Distances greater than 1 mile between two devices require long-range technologies. Wireless examples are cellular (2G, 3G, 4G) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies. LPWA communications have the ability to communicate over a large area without consuming much power. These technologies are therefore ideal for battery-powered IoT sensors. (LPWA and the other examples just mentioned are discussed in more detail later in this chapter.) Found mainly in industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications are classified as long range but are not really considered IoT access technologies. For more information on these standards, see http://standards.ieee.org/about/get/802/802.3.html and https://standards.ieee.org/findstds/standard/1901-2010.html.

For wireless deployments, the maximum coverage, as expressed in specifications or product descriptions, is often derived from optimal estimated conditions. In the real world, you should perform proper radio planning using the appropriate tools, followed by a field radio survey to better understand the actual conditions over a given area. You also need to consider environmental factors, such as interference and noise, and specific product characteristics such as antenna design and transmit power. Finally, you should be aware of potential landscape and topology changes in the field, such as new buildings, that may interfere with signal transmission.

Frequency Bands

Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC). These groups define the regulations and transmission requirements for various frequency bands. For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.

Around the world, the spectrum for various communications uses is often viewed as a critical resource. For example, you can see the value of these frequencies by examining the cost that mobile operators pay for licenses in the cellular spectrum.

Focusing on IoT access technologies, the frequency bands leveraged by wireless communications are split between licensed and unlicensed bands. Licensed spectrum is generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.

An important consideration for IoT access infrastructures that wish to utilize licensed spectrum is that users must subscribe to services when connecting their IoT devices. This adds more complexity to a deployment involving large numbers of sensors and other IoT devices, but in exchange for the subscription fee, the network operator can guarantee the exclusivity of the frequency usage over the target area and can therefore sell a better guarantee of service.

Improvements have been made in handling the complexity that is inherent when deploying large numbers of devices in the licensed spectrum. Thanks to the development of IoT platforms, such as the Cisco Jasper Control Center, automating the provisioning, deployment, and management of large numbers of devices has become much easier. Examples of licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.

Note Exceptions exist in the licensed spectrum. For example, the Digital Enhanced Cordless Telecommunications (DECT) wireless technology operates in licensed bands centered on 1.9 GHz, but no royalty fees apply. Therefore, DECT Ultra Low Energy (ULE) is defined as an IoT wireless communication standard in the licensed spectrum, but it does not require a service provider.

The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands. These frequencies are used in many communications technologies for short-range devices (SRDs). *Unlicensed* means that no guarantees or protections are offered in the ISM bands for device communications. For IoT access, these are the most well-known ISM bands:

- 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
- IEEE 802.15.1 Bluetooth
- IEEE 802.15.4 WPAN

Note The low range of IEEE 802.15.1 Bluetooth limits its usefulness in most IoT deployments.

An unlicensed band, such as those in the ISM range of frequencies, is not *unregulated*. National and regional regulations exist for each of the allocated frequency bands (much as with the licensed bands). These regulations mandate device compliance on parameters such as transmit power, duty cycle and dwell time, channel bandwidth, and channel hopping.

Unlicensed spectrum is usually simpler to deploy than licensed because it does not require a service provider. However, it can suffer from more interference because other devices may be competing for the same frequency in a specific area. This becomes a key element in decisions for IoT deployments. Should an IoT infrastructure utilize unlicensed spectrum available for private networks or licensed frequencies that are dependent on a service provider? Various LPWA technologies are taking on a greater importance when it comes to answering this question. In addition to meeting low power requirements, LPWA communications are able to cover long distances that in the past required the licensed bands offered by service providers for cellular devices.

Some communications within the ISM bands operate in the sub-GHz range. Sub-GHz bands are used by protocols such as IEEE 802.15.4, 802.15.4g, and 802.11ah, and LPWA technologies such as LoRa and Sigfox. (All these technologies are discussed in more detail later in this chapter.)

The frequency of transmission directly impacts how a signal propagates and its practical maximum range. (Range and its importance to IoT access are discussed earlier in this chapter.) Either for indoor or outdoor deployments, the sub-GHz frequency bands allow greater distances between devices. These bands have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles, while keeping the transmit power within regulation.

The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies. However, most IoT sensors do not need to send data at high rates. Therefore, the lower transmission speeds of sub-GHz technologies are usually not a concern for IoT sensor deployments.

For example, in most European countries, the 169 MHz band is often considered best suited for wireless water and gas metering applications. This is due to its good deep building basement signal penetration. In addition, the low data rate of this frequency matches the low volume of data that needs to be transmitted.

Several sub-GHz ranges have been defined in the ISM band. The most well-known ranges are centered on 169 MHz, 433 MHz, 868 MHz, and 915 MHz. However, most IoT access technologies tend to focus on the two sub-GHz frequency regions around 868 MHz and 915 MHz. These main bands are commonly found throughout the world and are applicable to nearly all countries.

Note Countries may also specify other unlicensed bands. For example, China has provisioned the 779–787 MHz spectrum as documented in the LoRaWAN 1.0 specifications and IEEE 802.15.4g standard.

The European Conference of Postal and Telecommunications Administrations (CEPT), in the European Radiocommunications Committee (ERC) Recommendation 70-03, defines the 868 MHz frequency band. CEPT was established in 1959 as a coordinating body for European state telecommunications and postal organizations. European countries generally apply Recommendation 70-03 to their national telecommunications regulations, but the 868 MHz definition is also applicable to regions and countries outside Europe. For example, India, the Middle East, Africa, and Russia have adopted the CEPT definitions, some of them making minor revisions. Recommendation 70-03 mostly characterizes the use of the 863–870 MHz band, the allowed transmit power, or EIRP (effective isotropic radiated power), and duty cycle (that is, the percentage of time a device can be active in transmission). EIRP is the amount of power that an antenna would emit to produce the peak power density observed in the direction of maximum antenna gain. The 868 MHz band is applicable to IoT access technologies such as IEEE 802.15.4 and 802.15.4g, 802.11ah, and LoRaWAN. (These protocols are covered later in this chapter.)

Note In the latest version of ERC Recommendation 70-03 (from May 2015), CEPT introduced the new frequency band 870–876 MHz. This band is relevant to IoT wireless access solutions. However, its adoption in local country regulations is still an ongoing process. This new band is referenced in the IEEE 802.15.4v draft and the Wi-SUN 1.0 regional PHY layer parameters. (Wi-SUN 1.0 is discussed later in this chapter.)

Centered on 915 MHz, the 902–928 MHz frequency band is the main unlicensed sub-GHz band available in North America, and it conforms to FCC regulations (FCC-Part-15.247). Countries around the world that do not align on the CEPT ERC 70-03 recommendation generally endorse the use of the 902–928 MHz range or a subset of it in their national regulations. For example, Brazilian regulator ANATEL defines the use of 902–907.5 and 915–928 MHz ranges (ANATEL506), the Japanese regulator ARIB provisions the 920–928 MHz range (ARIB-T108), and in Australia, ACMA provides recommendations for the 915–928 MHz range. As mentioned previously, even though these bands are unlicensed, they are regulated. The regulators document parameters, such as channel bandwidth, channel hopping, transmit power or EIRP, and dwell time.

In summary, you should take into account the frequencies and corresponding regulations of a country when implementing or deploying IoT smart objects. Smart objects running over unlicensed bands can be easily optimized in terms of hardware supporting the two main worldwide sub-GHz frequencies, 868 MHz and 915 MHz. However, parameters such as transmit power, antennas, and EIRP must be properly designed to follow the settings required by each country's regulations.

Power Consumption

While the definition of *IoT device* is very broad, there is a clear delineation between powered nodes and battery-powered nodes. A powered node has a direct connection to a power source, and communications are usually not limited by power consumption criteria. However, ease of deployment of powered nodes is limited by the availability of a power source, which makes mobility more complex.

Battery-powered nodes bring much more flexibility to IoT devices. These nodes are often classified by the required lifetimes of their batteries. Does a node need 10 to 15 years of battery life, such as on water or gas meters? Or is a 5- to 7-year battery life sufficient for devices such as smart parking sensors? Their batteries can be changed or the devices replaced when a street gets resurfaced. For devices under regular maintenance, a battery life of 2 to 3 years is an option.

IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes. This has led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA). Obviously, it is possible to run just about any wireless technology on batteries. However, in reality, no operational deployment will be acceptable if hundreds of batteries must be changed every month.

Wired IoT access technologies consisting of powered nodes are not exempt from power optimization. In the case of deployment of smart meters over PLC, the radio interface on meters can't consume 5 to 10 watts of power, or this will add up to a 20-million-meter deployment consuming 100 to 200 megawatts of energy for communications.

Topology

Among the access technologies available for connecting IoT devices, three main topology schemes are dominant: star, mesh, and peer-to-peer. For long-range and short-range technologies, a star topology is prevalent, as seen with cellular, LPWA, and Bluetooth networks. Star topologies utilize a single central base station or controller to allow communications with endpoints.

For medium-range technologies, a star, peer-to-peer, or mesh topology is common, as shown in Figure 4-2. Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other. Obviously, peer-to-peer topologies rely on multiple full-function devices. Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.

For example, indoor Wi-Fi deployments are mostly a set of nodes forming a star topology around their access points (APs). Meanwhile, outdoor Wi-Fi may consist of a mesh topology for the backbone of APs, with nodes connecting to the APs in a star topology. Similarly, IEEE 802.15.4 and 802.15.4g and even wired IEEE 1901.2a PLC are generally deployed as a mesh topology. A mesh topology helps cope with low transmit power, searching to reach a greater overall distance, and coverage by having intermediate nodes relaying traffic for other nodes.

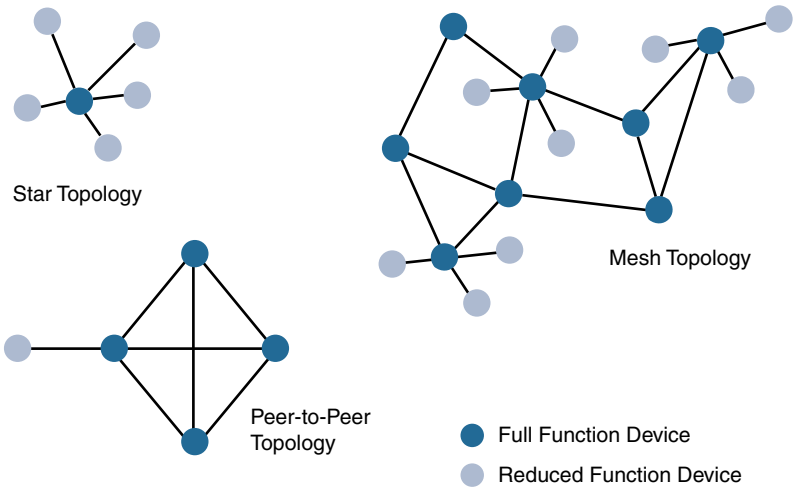


Figure 4-2 *Star, Peer-to-Peer, and Mesh Topologies*

Mesh topology requires the implementation of a Layer 2 forwarding protocol known as *mesh-under* or a Layer 3 forwarding protocol referred to as *mesh-over* on each intermediate node. (See Chapter 5, "IP as the IoT Network Layer," for more information.) As discussed previously in Chapter 2, "IoT Network Architecture and Design," an intermediate node or full-function device (FFD) is simply a node that interconnects other nodes. A node that doesn't interconnect or relay the traffic of other nodes is known as a leaf node, or reduced-function device (RFD). (More information on full-function and reduced-function devices is also presented later in this chapter.)

While well adapted to powered nodes, mesh topology requires a properly optimized implementation for battery-powered nodes. Battery-powered nodes are often placed in a "sleep mode" to preserve battery life when not transmitting. In the case of mesh topology, either the battery-powered nodes act as leaf nodes or as a "last resource path" to relay traffic when used as intermediate nodes. Otherwise, battery lifetime is greatly shortened. For battery-powered nodes, the topology type and the role of the node in the topology (for example, being an intermediate or leaf node) are significant factors for a successful implementation.

Constrained Devices

The Internet Engineering Task Force (IETF) acknowledges in RFC 7228 that different categories of IoT devices are deployed. While categorizing the class of IoT nodes is a perilous exercise, with computing, memory, storage, power, and networking continuously evolving and improving, RFC 7228 gives some definitions of constrained nodes. These definitions help differentiate constrained nodes from unconstrained nodes, such as servers, desktop or laptop computers, and powerful mobile devices such as smart phones.

Constrained nodes have limited resources that impact their networking feature set and capabilities. Therefore, some classes of IoT nodes do not implement an IP stack. According to RFC 7228, constrained nodes can be broken down into the classes defined in Table 4-1.

Table 4-1 *Classes of Constrained Nodes, as Defined by RFC 7228*

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.

Class	Definition
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

Constrained-Node Networks

While several of the IoT access technologies, such as Wi-Fi and cellular, are applicable to laptops, smart phones, and some IoT devices, some IoT access technologies are more suited to specifically connect constrained nodes. Typical examples are IEEE 802.15.4 and 802.15.4g RF, IEEE 1901.2a PLC, LPWA, and IEEE 802.11ah access technologies. (These technologies are discussed in more detail later in this chapter.)

Constrained-node networks are often referred to as low-power and lossy networks (LLNs). (See Chapter 5 for more details on LLNs.) *Low-power* in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes. *Lossy networks* indicates that network performance may suffer from interference and variability due to harsh radio environments. Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability: data rate and throughput, latency and determinism, and overhead and payload.

Data Rate and Throughput

The data rates available from IoT access technologies range from 100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac. (Sigfox, LTE, and IEEE 802.11ac are discussed later in this chapter.) However, the actual throughput is less—sometimes much less—than the data rate. Therefore, understanding the bandwidth requirements of a particular technology, its applicability to given use cases, the capacity planning rules, and the expected real throughput are important for proper network design and successful production deployment.

Technologies not particularly designed for IoT, such as cellular and Wi-Fi, match up well to IoT applications with high bandwidth requirements. For example, nodes involved with video analytics have a need for high data rates. These nodes are found in retail, airport,

and smart cities environments for detecting events and driving actions. Because these types of IoT endpoints are not constrained in terms of computing or network bandwidth, the design guidelines tend to focus on application requirements, such as latency and determinism. (Latency and determinism is discussed in more detail later in this chapter.)

Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints. For example, Bluetooth sensors that are now appearing on connected wearables fall into this category. In this case, the solutions focus more on footprint and battery lifetime than on data rate.

The IoT access technologies developed for constrained nodes are optimized for low power consumption, but they are also limited in terms of data rate, which depends on the selected frequency band, and throughput.

With the data rate ranging from 100 bps to less than 1 Mbps, you may think back to the years when bandwidth was a scarce resource. You often needed some expertise to understand how to design such networks. Today this sort of expertise is helpful for LPWA networks, which are designed with a certain number of messages per day or per endpoint rather than just having a pure bandwidth usage limit in place. In addition, in an access mesh topology, an application's behavior, such as frequency polling, impacts the design because all devices share the constrained bandwidth capacity.

A discussion of data rate and bandwidth in LLNs must include a look at real throughput, or "goodput," as seen by the application. While it may not be important for constrained nodes that send only one message a day, real throughput is often very important for constrained devices implementing an IP stack. In this case, throughput is a lower percentage of the data rate, even if the node gets the full constrained network at a given time.

For example, let's consider an IEEE 802.15.4g subnetwork implementing 2FSK modulation at 150 kbps for the 915 MHz frequency band. (The IEEE 802.15.4g protocol is covered in more detail later in this chapter.) To cover the border case of distance and radio signal quality, Forward Error Correction (FEC) will be turned on, which lowers the data rate from 150 kbps to 75 kbps. If you now add in the protocol stack overhead, the two-way communication handling, and the variable data payload size, you end up with a maximum throughput of 30 to 40 kbps. This must be considered as the best value because the number of devices simultaneously communicating along with the topology and control plane overhead will also impact the throughput.

Another characteristic of IoT devices is that a majority of them initiate the communication. Upstream traffic toward an application server is usually more common than downstream traffic from the application server. Understanding this behavior also helps when deploying an IoT access technology, such as cellular, that is asymmetrical because the upstream bandwidth must be considered a key parameter for profiling the network capacity.

Latency and Determinism

Much like throughput requirements, latency expectations of IoT applications should be known when selecting an access technology. This is particularly true for wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviors.

On constrained networks, latency may range from a few milliseconds to seconds, and applications and protocol stacks must cope with these wide-ranging values. For example, UDP at the transport layer is strongly recommended for IP endpoints communicating over LLNs. In the case of mesh topologies, if communications are needed between two devices inside the mesh, the forwarding path may call for some routing optimization, which is available using the IPv6 RPL protocol. (For more information on RPL, see Chapter 5.)

Note When latency is a strong concern, emergent access technologies such as Deterministic Ethernet or the Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e should be considered. However, some of these solutions are not fully mature for production deployment. (For more information on TSCH, see Chapter 5. The 802.15.4e protocol is discussed later in this chapter.)

Overhead and Payload

When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications. In addition, you should be aware of any requirements for IP. The minimum IPv6 MTU size is expected to be 1280 bytes. Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs.

Note The use of IP on IoT devices is an open topic of discussion. As mentioned earlier in this chapter, the IETF acknowledges the fact that different classes of IoT devices exist. For the more constrained classes of devices, like Class 0 and Class 1 devices, it is usually not possible or optimal to implement a complete IP stack implementation.

For technologies that fall under the LLN definition but are able to transport IP, such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization is important. (The protocols IEEE 802.14 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah are covered later in this chapter.) For example, the payload size for IEEE 802.15.4 is 127 bytes and requires an IPv6 payload with a minimum MTU of 1280 bytes to be fragmented. (For more information on the fragmentation of IPv6, see Chapter 5.) On the other hand, IEEE 802.15.4g enables payloads up to 2048 bytes, easing the support of the IPv6 minimum MTU of 1280 bytes.

Most LPWA technologies offer small payload sizes. These small payload sizes are defined to cope with the low data rate and time over the air or duty cycle requirements of IoT nodes and sensors. For example, payloads may be as little as 19 bytes using LoRaWAN technology or up to 250 bytes, depending on the adaptive data rate (ADR). While this doesn't preclude the use of an IPv6/6LoWPAN payload, as seen on some endpoint implementations, these types of protocols are better suited to Class 0 and 1 nodes, as defined in RFC 7228. (LoRaWAN and ADR are discussed in more detail later in this chapter. RFC 7228 and the node classes it defines are covered earlier in this chapter.)

In conclusion, the communication criteria just covered are fundamental to understanding IoT access technologies, their characteristics, and when they are most applicable. These criteria include range, frequency bands, power consumption, network topology, the presence of constrained devices and/or networks, and data throughput.

From a network engineer perspective, you must make sure an architecture is developed with the proper abstraction for a particular access technology. This is especially true for constrained network nodes, where quite often your choices of protocols and solutions can be limited. The next section reviews the main IoT access technologies dedicated to constrained networks.

IoT Access Technologies

The previous section describes criteria that help you in evaluating IoT constrained network technologies for proper design and operations. This section provides an overview of the main IoT access technologies. The technologies highlighted here are the ones that are seen as having market and/or mind share. Therefore, you should have a basic familiarity with them as they are fundamental to many IoT conversations.

Note Remember that there are many more IoT technologies in the market today than we can discuss here. This chapter focuses on the ones that appear to have the strongest foothold.

For each of the IoT access technologies discussed in this chapter, a common information set is being provided. Particularly, the following topics are addressed for each IoT access technology:

- **Standardization and alliances:** The standards bodies that maintain the protocols for a technology
- **Physical layer:** The wired or wireless methods and relevant frequencies
- **MAC layer:** Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control
- **Topology:** The topologies supported by the technology
- **Security:** Security aspects of the technology
- **Competitive technologies:** Other technologies that are similar and may be suitable alternatives to the given technology

While having a familiarity with these protocols and their capabilities is recommended, you may find that much of the information about these technologies is better used as reference material. When you encounter these protocols, you can use this chapter as a handy overview and quick summary of the important details.

IEEE 802.15.4

IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries. In addition to being low cost and offering a reasonable battery life, this access technology enables easy installation using a compact protocol stack while remaining both simple and flexible. Several network communication stacks, including deterministic ones, and profiles leverage this technology to address a wide range of IoT use cases in both the consumer and business markets. IEEE 802.15.4 is commonly found in the following types of deployments:

- Home and building automation
- Automotive networks
- Industrial wireless sensor networks
- Interactive toys and remote controls

Criticisms of IEEE 802.15.4 often focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading. The negatives around reliability and latency often have to do with the Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm. CSMA/CA is an access method in which a device "listens" to make sure no other devices are transmitting before starting its own transmission. If another device is transmitting, a wait time (which is usually random) occurs before "listening" occurs again. Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique. Later variants of 802.15.4 from the IEEE start to address these issues. (See the section "IEEE 802.15.4e and 802.15.4g," later in this chapter, for more information.)

Note Most forms of radio communications are affected by multipath fading to varying degrees. *Multipath fading* refers to multiple copies of the signal hitting the receiver at different points in time because of different signal paths and reflections. The ability to change frequencies can mitigate the effects of multipath fading.

Standardization and Alliances

IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN). This standard has evolved over the years and is a well-known solution for low-complexity wireless devices with low data rates that need many months or even years of battery life. For more detailed information on IEEE 802.15.4, visit www.ieee802.org/15/pub/TG4.html.

Since 2003, the IEEE has published several iterations of the IEEE 802.15.4 specification, each labeled with the publication's year. For example, IEEE 802.15.4-2003 was published in 2003, 802.15.4-2006 was released in 2006, and 802.15.4-2011 and 802.15.4-2015 were issued in 2011 and 2015, respectively. Newer releases typically supersede older ones, integrate addendums, and add features or clarifications to previous versions.

While there is no alliance or promotion body for IEEE 802.15.4 per se, the IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks. These protocol stacks make use of 802.15.4 at the physical and link layer levels, but the upper layers are different. These protocol stacks are promoted separately through various organizations and often commercialized. Some of the most well-known protocol stacks based on 802.15.4 are highlighted in Table 4-2.

Table 4-2 *Protocol Stacks Utilizing IEEE 802.15.4*

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

Because of its relatively long history compared to the others, ZigBee is one of the most well-known protocols listed in Table 4-2. In addition, ZigBee has continued to evolve over time as evidenced by the release of Zigbee IP and is representative of how IEEE 802.15.4 can be leveraged at the PHY and MAC layers, independent of the protocol layers above. For these reasons, both Zigbee and Zigbee IP are discussed in more detail in the following sections.

ZigBee

Based on the idea of ZigBee-style networks in the late 1990s, the first ZigBee specification was ratified in 2004, shortly after the release of the IEEE 802.15.4 specification the previous year. While not released as a typical standard, like an RFC, ZigBee still had industry support from more than 100 companies upon its initial publication. This industry support has grown to more than 400 companies that are members of the ZigBee Alliance. Similar to the Wi-Fi Alliance, the Zigbee Alliance is an industry group formed to certify interoperability between vendors and it is committed to driving and evolving ZigBee as an IoT solution for interconnecting smart objects.

ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs. Furthermore, products that are ZigBee compliant and certified by the ZigBee Alliance should interoperate even though different vendors may manufacture them.

The Zigbee specification has undergone several revisions. In the 2006 revision, sets of commands and message types were introduced, and increased in number in the 2007 (called Zigbee pro) iteration, to achieve different functions for a device, such as metering, temperature, or lighting control. These sets of commands and message types are called clusters. Ultimately, these clusters from different functional domains or libraries form the building blocks of Zigbee application profiles. Vendors implementing pre-defined Zigbee application profiles like Home Automation or Smart Energy can ensure interoperability between their products.

The main areas where ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy. In the industrial and commercial automation space, ZigBee-based devices can handle various functions, from measuring temperature and humidity to tracking assets. For home automation, ZigBee can control lighting, thermostats, and security functions. ZigBee Smart Energy brings together a variety of interoperable products, such as smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water. These ZigBee products are controlled by the utility provider and can help coordinate usage between homes and businesses and the utility provider itself to provide more efficient operations.

The traditional ZigBee stack is illustrated in Figure 4-3. As mentioned previously, ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers. (The 802.15.4 PHY and MAC layers are covered in detail later in this chapter.) ZigBee specifies the network and security layer and application support layer that sit on top of the lower layers.

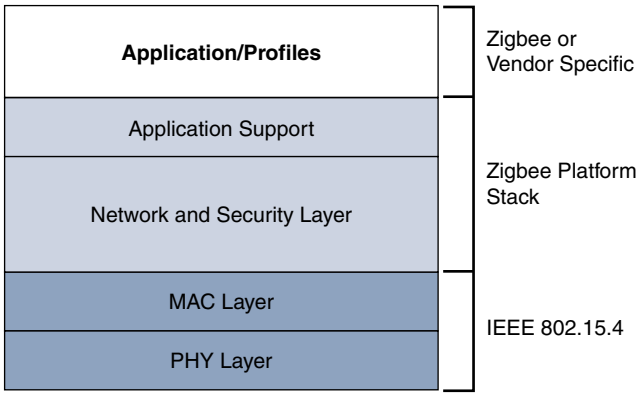


Figure 4-3 *High-Level ZigBee Protocol Stack*

The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications. This includes calculating routing paths in what is often a changing topology, discovering neighbors, and managing the routing tables as devices join for the first time. The network layer is also responsible for forming the appropriate topology, which is often a mesh but could be a star or tree as well. From a security perspective, ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.

Note ZigBee uses Ad hoc On-Demand Distance Vector (AODV) routing across a mesh network. Interestingly, this routing algorithm does not send a message until a route is needed. Assuming that the next hop for a route is not in its routing table, a network node broadcasts a request for a routing connection. This causes a burst of routing-related traffic, but after a comparison of various responses, the path with the lowest number of hops is determined for the connection. This process is quite different from standard enterprise routing protocols, which usually learn the entire network topology in some manner and then store a consolidated but complete routing table.

The application support layer in Figure 4-3 interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications. ZigBee predefines many application profiles for certain industries, and vendors can optionally create their own custom ones at this layer. As mentioned previously, Home Automation and Smart Energy are two examples of popular application profiles.

ZigBee is one of the most well-known protocols built on an IEEE 802.15.4 foundation. On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles. While this structure has provided a fair degree of interoperability for vendors with membership in the ZigBee Alliance, it has not provided interoperability with other IoT solutions. However, this has started to change with the release of ZigBee IP, which is discussed next.

ZigBee IP

With the introduction of ZigBee IP, the support of IEEE 802.15.4 continues, but the IP and TCP/UDP protocols and various other open standards are now supported at the network and transport layers. The ZigBee-specific layers are now found only at the top of the protocol stack for the applications.

ZigBee IP was created to embrace the open standards coming from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL. (These IETF standards are discussed in Chapter 5.) They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.

ZigBee IP is a critical part of the Smart Energy (SE) Profile 2.0 specification from the ZigBee Alliance. SE 2.0 is aimed at smart metering and residential energy management systems. In fact, ZigBee IP was designed specifically for SE 2.0 but it is not limited to this use case. Any other applications that need a standards-based IoT stack can utilize Zigbee IP. The ZigBee IP stack is shown in Figure 4-4.

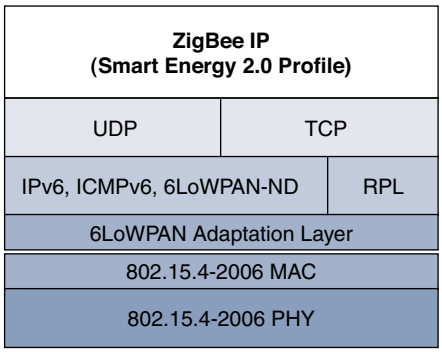


Figure 4-4 *ZigBee IP Protocol Stack*

Unlike traditional ZigBee, discussed in the previous section, ZigBee IP supports 6LoWPAN as an adaptation layer. (The 6LoWPAN protocol is covered in Chapter 5.) The 6LoWPAN mesh addressing header is not required as ZigBee IP utilizes the mesh-over or route-over method for forwarding packets. ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes.

At the network layer, all ZigBee IP nodes support IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND), and utilize RPL for the routing of packets across the mesh network. IPv6 and RPL are discussed in more detail in Chapter 5. Both TCP and UDP are also supported, to provide both connection-oriented and connectionless service.

As you can see, ZigBee IP is a compelling protocol stack offering because it is based on current IoT standards at every layer under the application layer. This opens up opportunities for ZigBee IP to integrate and interoperate on just about any 802.15.4 network with other solutions built on these open IoT standards. The following sections take a deeper dive into 802.15.4 and its PHY and MAC layers.

Physical Layer

The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands. (ISM bands are discussed earlier in this chapter.) The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation. DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth. The original physical layer transmission options were as follows:

- 2.4 GHz, 16 channels, with a data rate of 250 kbps
- 915 MHz, 10 channels, with a data rate of 40 kbps
- 868 MHz, 1 channel, with a data rate of 20 kbps

You should note that only the 2.4 GHz band operates worldwide. The 915 MHz band operates mainly in North and South America, and the 868 MHz frequencies are used in Europe, the Middle East, and Africa. IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following:

- **OQPSK PHY:** This is DSSS PHY, employing offset quadrature phase-shift keying (OQPSK) modulation. OQPSK is a modulation technique that uses four unique bit values that are signaled by phase changes. An offset function that is present during phase shifts allows data to be transmitted more reliably.
- **BPSK PHY:** This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation. BPSK specifies two unique phase shifts as its data encoding scheme.
- **ASK PHY:** This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation. PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS. ASK uses amplitude shifts instead of phase shifts to signal different bit values.

These improvements increase the maximum data rate for both 868 MHz and 915 MHz to 100 kbps and 250 kbps, respectively. The 868 MHz support was enhanced to 3 channels, while other IEEE 802.15.4 study groups produced addendums for new frequency bands. For example, the IEEE 802.15.4c study group created the bands 314–316 MHz, 430–434 MHz, and 779–787 MHz for use in China.

Figure 4-5 shows the frame for the 802.15.4 physical layer. The synchronization header for this frame is composed of the Preamble and the Start of Frame Delimiter fields. The Preamble field is a 32-bit 4-byte (for parallel construction) pattern that identifies the start of the frame and is used to synchronize the data transmission. The Start of Frame Delimiter field informs the receiver that frame contents start immediately after this byte.

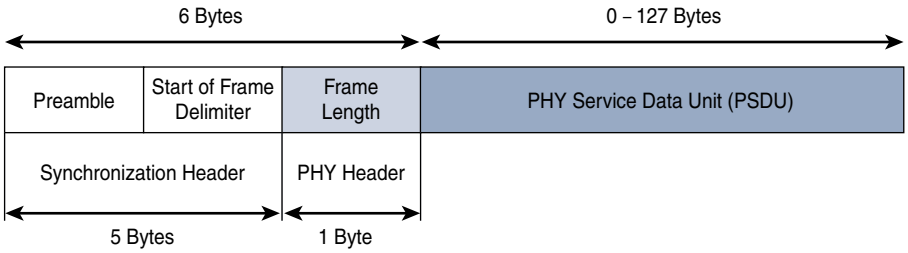


Figure 4-5 *IEEE 802.15.4 PHY Format*

The PHY Header portion of the PHY frame shown in Figure 4-5 is simply a frame length value. It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY. The PSDU is the data field or payload.

Note The maximum size of the IEEE 802.15.4 PSDU is 127 bytes. This size is significantly smaller than the lowest MTU setting of other upper-layer protocols, such as IPv6, which has a minimum MTU setting of 1280 bytes. Therefore, fragmentation of the IPv6 packet must occur at the data link layer for larger IPv6 packets to be carried over IEEE 802.15.4 frames. (See Chapter 5 for more details.)

The various versions and addendums to 802.15.4 over the years through various working groups can make it somewhat difficult to follow. Therefore, you should pay attention to which versions of 802.15.4 particular devices support. Products and solutions must refer to the proper IEEE 802.15.4 specification, frequency band, modulation, and data rate when providing details on their physical layer implementation.

MAC Layer

The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated. At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer performs the following tasks:

- Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
- PAN association and disassociation by a device
- Device security
- Reliable link communications between two peer MAC entities

The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of MAC frames are specified in 802.15.4:

- **Data frame:** Handles all transfers of data
- **Beacon frame:** Used in the transmission of beacons from a PAN coordinator

- **Acknowledgement frame:** Confirms the successful reception of a frame
- **MAC command frame:** Responsible for control communication between devices

Each of these four 802.15.4 MAC frame types follows the frame format shown in Figure 4-6. In Figure 4-6, notice that the MAC frame is carried as the PHY payload. The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.

The MAC Header field is composed of the Frame Control, Sequence Number and the Addressing fields. The Frame Control field defines attributes such as frame type, addressing modes, and other control flags. The Sequence Number field indicates the sequence identifier for the frame. The Addressing field specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields.

Note Within the Frame Control portion of the 802.15.4 header is the Security Enabled field. When this field is set to a value of 0, the frame format matches Figure 4-6. Beginning with the 802.15.4-2006 specification, when this field is set to a value of 1, an Auxiliary Security Header field is added to the 802.15.4 frame, as shown later, in Figure 4-8.

The MAC Payload field varies by individual frame type. For example, beacon frames have specific fields and payloads related to beacons, while MAC command frames have different fields present. The MAC Footer field is nothing more than a frame check sequence (FCS). An FCS is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the data in the frame.

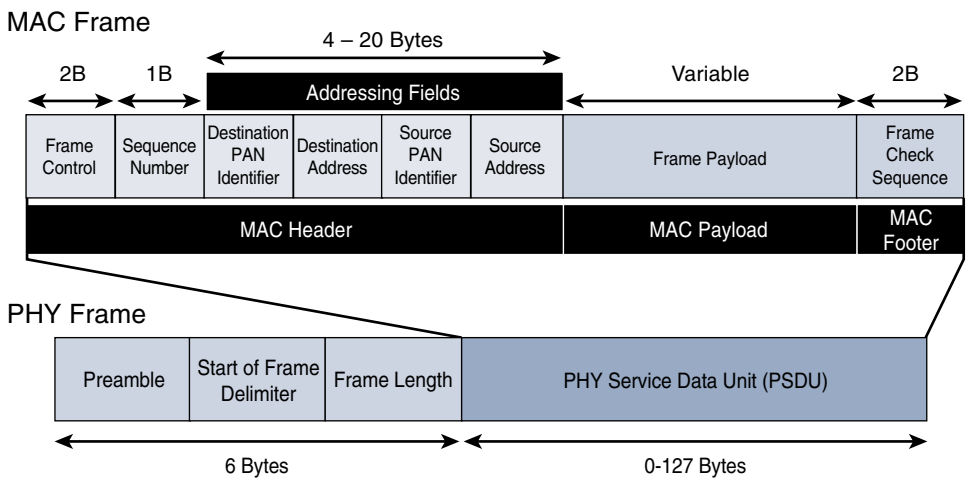


Figure 4-6 *IEEE 802.15.4 MAC Format*

IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address, based on EUI-64. However, because the maximum payload is 127 bytes, 802.15.4 also defines how a 16-bit "short address" is assigned to devices. This short address is local to

the PAN and substantially reduces the frame overhead compared to a 64-bit extended MAC address. However, you should be aware that the use of this short address might be limited to specific upper-layer protocol stacks.

Topology

IEEE 802.15.4–based networks can be built as star, peer-to-peer, or mesh topologies. Mesh networks tie together many nodes. This allows nodes that would be out of range if trying to communicate directly to leverage intermediary nodes to transfer communications.

Please note that every 802.15.4 PAN should be set up with a unique ID. All the nodes in the same 802.15.4 network should use the same PAN ID. Figure 4-7 shows an example of an 802.15.4 mesh network with a PAN ID of 1.

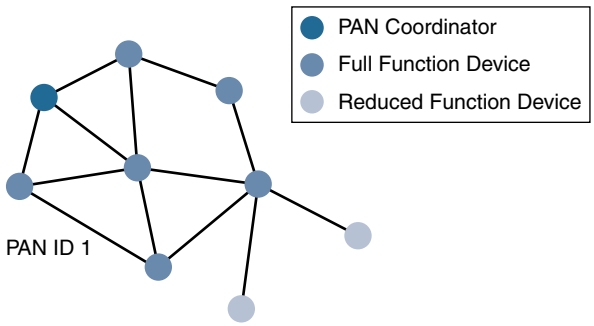


Figure 4-7 *802.15.4 Sample Mesh Network Topology*

As mentioned earlier in this chapter, full-function devices (FFDs) and reduced-function devices (RFDs) are defined in IEEE 802.15.4. A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN. Notice in Figure 4-7 that a single PAN coordinator is identified for PAN ID 1. FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology. This function can be done at Layer 2 and is known as *mesh-under*. Generally, this is based on a proprietary solution. Alternatively, the routing function can occur at Layer 3, using a routing protocol, such as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). This is referred to as *mesh-over*. (To learn more about mesh-under, mesh-over, and RPL, see Chapter 5.)

Security

The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data. Established by the US National Institute of Standards and Technology in 2001, AES is a block cipher,

which means it operates on fixed-size blocks of data. The use of AES by the US government and its widespread adoption in the private sector has helped it become one of the most popular algorithms used in symmetric key cryptography. (A *symmetric key* means that the same key is used for both the encryption and decryption of the data.)

In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent. This is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption.

Enabling these security features for 802.15.4 changes the frame format slightly and consumes some of the payload. Using the Security Enabled field in the Frame Control portion of the 802.15.4 header is the first step to enabling AES encryption. This field is a single bit that is set to 1 for security. Once this bit is set, a field called the Auxiliary Security Header is created after the Source Address field, by stealing some bytes from the Payload field. Figure 4-8 shows the IEEE 802.15.4 frame format at a high level, with the Security Enabled bit set and the Auxiliary Security Header field present.

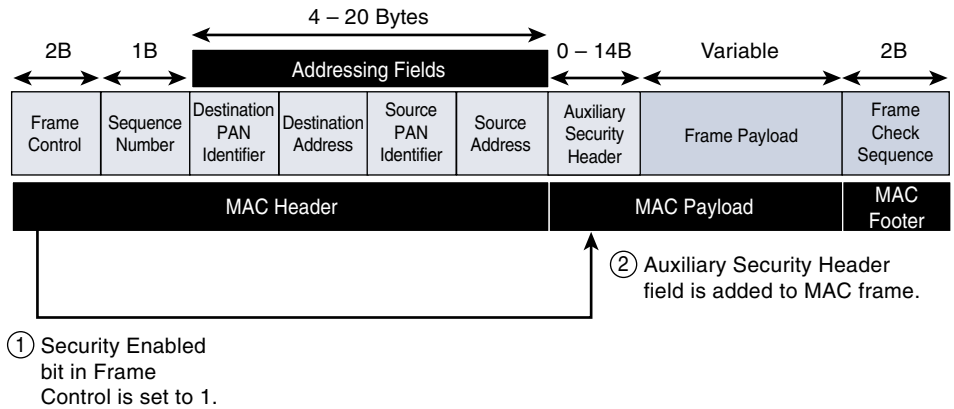


Figure 4-8 *Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions*

Competitive Technologies

As detailed in Table 4-2, the IEEE 802.15.4 PHY and MAC layers are the foundations for several networking profiles that compete against each other in various IoT access environments. These various vendors and organizations build upper-layer protocol stacks on top of an 802.15.4 core. They compete and distinguish themselves based on features and capabilities in these upper layers.

A competitive radio technology that is different in its PHY and MAC layers is DASH7. DASH7 was originally based on the ISO18000-7 standard and positioned for industrial communications, whereas IEEE 802.15.4 is more generic. Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military

forces for many years, mainly for logistics purposes. Active RFID utilizes radio waves generated by a battery-powered tag on an object to enable continuous tracking.

The current DASH7 technology offers low power consumption, a compact protocol stack, range up to 1 mile, and AES encryption. Frequencies of 433 MHz, 868 MHz, and 915 MHz have been defined, enabling data rates up to 166.667 kbps and a maximum payload of 256 bytes.

DASH7 is promoted by the DASH7 Alliance, which has evolved the protocol from its active RFID niche into a wireless sensor network technology that is aimed at the commercial market. For more information on DASH7, see the Dash7 Alliance webpage, at www.dash7-alliance.org.

IEEE 802.15.4 Conclusions

The IEEE 802.15.4 wireless PHY and MAC layers are mature specifications that are the foundation for various industry standards and products (refer to Table 4-2). The PHY layer offers a maximum speed of up to 250 kbps, but this varies based on modulation and frequency. The MAC layer for 802.15.4 is robust and handles how data is transmitted and received over the PHY layer. Specifically, the MAC layer handles the association and disassociation of devices to/from a PAN, reliable communications between devices, security, and the formation of various topologies.

The topologies used in 802.15.4 include star, peer-to-peer, and cluster trees that allow for the formation of mesh networks. From a security perspective, 802.15.4 utilizes AES encryption to allow secure communications and also provide data integrity.

The main competitor to IEEE 802.15.4 is DASH7, another wireless technology that compares favorably. However, IEEE 802.15.4 has an edge in the marketplace through all the different vendors and organizations that utilize its PHY and MAC layers. As 802.15.4 continues to evolve, you will likely see broader adoption of the IPv6 standard at the network layer. For IoT sensor deployments requiring low power, low data rate, and low complexity, the IEEE 802.15.4 standard deserves strong consideration.

IEEE 802.15.4g and 802.15.4e

The IEEE frequently makes amendments to the core 802.15.4 specification, before integrating them into the next revision of the core specification. When these amendments are made, a lowercase letter is appended. Two such examples of this are 802.15.4e-2012 and 802.15.4g-2012, both of which are especially relevant to the subject of IoT. Both of these amendments were integrated in IEEE 802.15.4-2015 but are often still referred to by their amendment names.

The IEEE 802.15.4e amendment of 802.15.4-2011 expands the MAC layer feature set to remedy the disadvantages associated with 802.15.4, including MAC reliability, unbounded latency, and multipath fading. In addition to making general enhancements to the MAC layer, IEEE 802.15.4e also made improvements to better cope with certain application domains, such as factory and process automation and smart grid. Smart grid

UNIT-3

UNIT II: IoT and M2M

The Vision-Introduction, From M2M to IoT, M2M towards IoT-the global context, A use case example, Differing Characteristics.**A Market Perspective**– Introduction, Some Definitions, M2M Value Chains, IoT Value Chains, An emerging industrial structure for IoT

The Vision

2.1 Introduction

- M2M, or machine-to-machine, is a direct communication between devices using wired or wireless communication channels.
- M2M refers to the interaction of two or more devices/machines that are connected to each other.
- Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction. uptake of both M2M and IoT solutions will increase dramatically.
- These devices capture data and share with other connected devices, creating an intelligent network of things or systems. Devices could be sensors, actuators, embedded systems or other connected elements.
- M2M technology could be present in our homes, offices, shopping malls and other places. Controlling electrical appliances like bulbs and fans using RF or Bluetooth from your smartphone is a simple example of M2M applications at home. Here, the electrical appliance and your smartphone are the two machines interacting with each other.
- The Internet of Things (IoT) is the network of physical devices embedded with sensors, software and electronics, enabling these devices to communicate with each other and exchange data over a computer network. The things in the IoT refer to hardware devices uniquely identifiable through a network platform within the Internet infrastructure.
- M2M and the IoT are two of the technologies that form the basis of the new world.
- Anything in the physical realm that is of interest to observe and control by people, businesses, or organizations will be connected and will offer services via the Internet.
- The physical entities can be of any nature, such as buildings, farmland, and natural resources like air, and even such personal real-world concepts as my favorite hiking route through the forest or my route to work.
- M2M is about machines, smartphones and appliances, whereas the IoT is about sensors, cyber-based physical systems, Internet and so on

---

2.2 From M2M to IoT

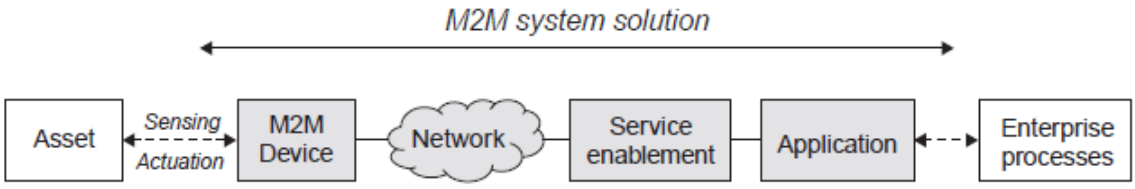
- M2M and IoT solutions will increase dramatically.
- **Reasons for using M2M and IoT**

1. An increased need for understanding the physical environment in its various forms, from industrial installations through to public spaces and consumer demands.
2. The improvement of technology
3. Improved networking capabilities.
4. Reduced costs of components and the ability to more cheaply collect and analyze the data they produce.

M2M communication

- M2M refers to those solutions that allow communication between devices of the same type and a specific application, all via wired or wireless communication networks.
- The term M2M communication describes devices which are connected to the internet using fixed/wireless networks and communicate with each other as well as with other devices on the network.
- M2M solutions allow end-users to capture data about events from assets, such as temperature or inventory levels.
- M2M can be used for sharing and storing information for administration and operational purposes, monitoring, diagnostics and notifications or alerts.
- M2M has been applied in many different scenarios, including the remote monitoring and control of enterprise assets, or to provide connectivity of remote machine-type devices.

Generic M2M Solution



- A typical M2M system solution consists of M2M devices, communication networks that provide remote connectivity for the devices, service enablement and application logic, and integration of the M2M application into the business processes provided by an Information Technology (IT) system of the enterprise.
- The M2M system solution is used to remotely monitor and control enterprise assets of various kinds, and to integrate those assets into the business processes of the enterprise in question. The asset can be of a wide range of types (e.g. vehicle, freight container, building, or smart electricity meter), all depending on the enterprise.
- The system components of an M2M solution are as follows:

• **M2M Device.**

- This is the M2M device attached to the asset of interest, and provides sensing and actuation capabilities.

• **Network.**

- The purpose of the network is to provide remote connectivity between the M2M device and the application-side servers. Many different network types can be used, and include both Wide Area Networks (WANs) and Local Area Networks (LANs), sometimes also referred to as Capillary Networks or M2M Area Networks.

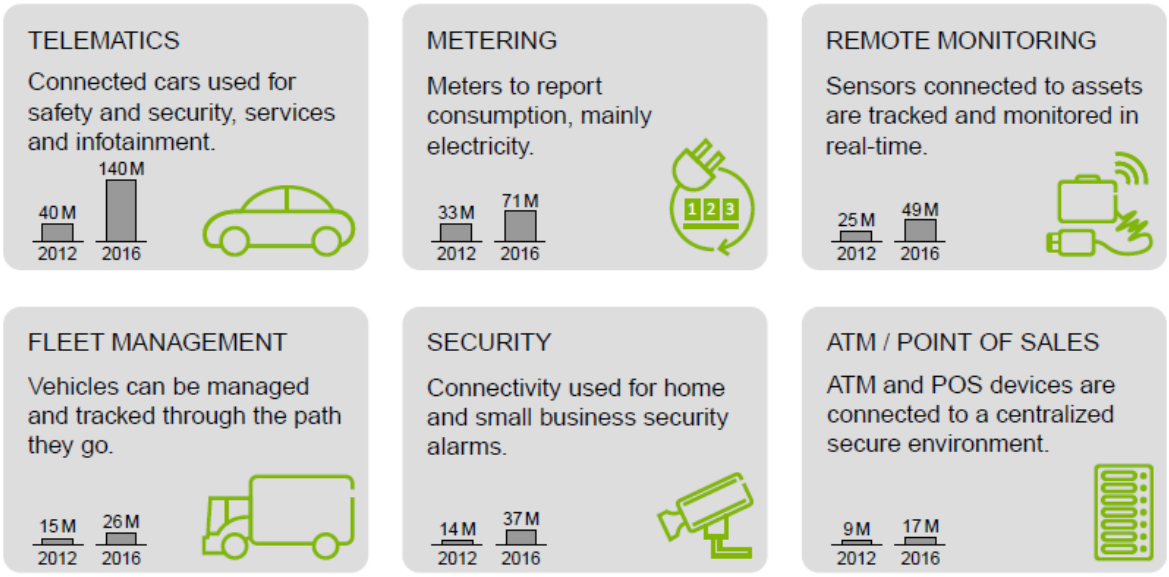
• M2M Service Enablement.

- This component provides generic functionality that is common across a number of different applications. Its primary purpose is to reduce cost for implementation and ease of application development.

• M2M Application.

- The application component of the solution is a realization of the highly specific monitor and control process. The application is further integrated into the overall business process system of the enterprise.

Key application areas



- Telematics for cars and vehicles. Typical applications include navigation, remote vehicle diagnostics pay-as-you-drive insurance schemes, road charging, and stolen vehicle recovery.
- Metering applications include primarily remote meter management and data collection for energy consumption in the electricity utility sector, but also for gas and water consumption.
- Remote monitoring is more generalized monitoring of assets, and includes remote patient monitoring as one prime example.
- Fleet management includes a number of different applications, like data logging, goods and vehicle positioning, and security of valuable or hazardous goods.

- Security applications are mainly those related to home alarms and small business surveillance solutions. The final market segment is Automated
- Teller Machines (ATM) and Point of Sales (POS) terminals.
- M2M communication requires availability of constant internet connection with reasonable speed.

Benefits or advantages of M2M Communication

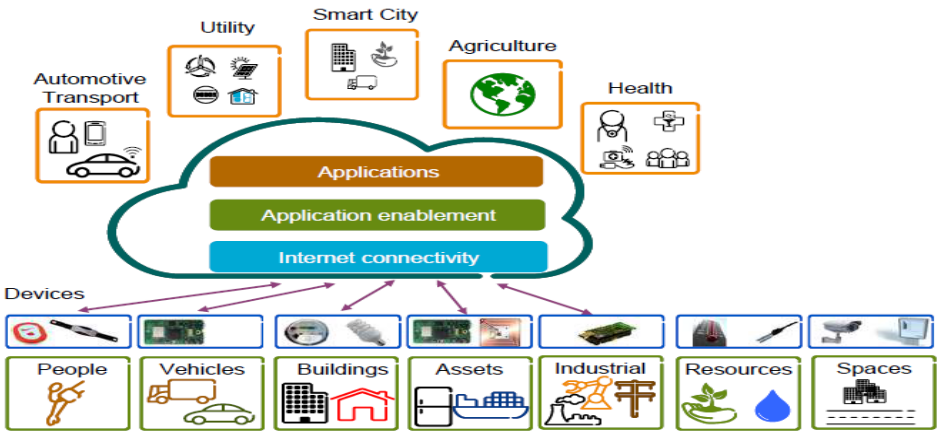
- M2M communication is supported by cellular networks either directly or through gateway.
- It is easy to roll out and maintain.
- It is available with fixed and mobile networks both indoors and outdoors.
- It offers higher range, minimum latency, higher throughput and consume less energy.
- It enables communication of smart devices without any human intervention.
- The security and privacy issues in IoT networks are resolved by using M2M communication facility.
- Large protection, data collection and data processing is possible.

Drawbacks or disadvantages of M2M Communication

- Use of cloud computing in M2M means dependence on others which could limit flexibility and innovation.
- Security and ownership of data is a big concern.
- Interoperability between cloud/M2M IoT devices is a big concern in such networks.
- It is designed and optimized for small number of network devices.

IoT

- connecting sensors and other devices to Information and Communication Technology (ICT) systems via wired or wireless networks.
- IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies.
- It allows things and real world objects to connect, communicate, and interact with one another in the same way humans do via the web today.
- Internet be only about people, media, and content,but it will also include all real-world assets as intelligent creatures exchanging information, interacting with people, supporting business processes of enterprises, and creating knowledge.
- It is an extension to the existing Internet.
- IoT is about the technology, the remote monitoring, and control, and also about where these technologies are applied.
- IoT applications will not only rely on data and services from sensor and actuators alone. Equally important is the blend-in of other information sources that have relevance from the viewpoint of the physical world.
- These can be data from Geographic Information Systems (GIS) like road databases and weather forecasting systems.



- Even information extracted from social media like Twitter feeds or Facebook status updates that relate to real world observations can be fed into the same IoT system.

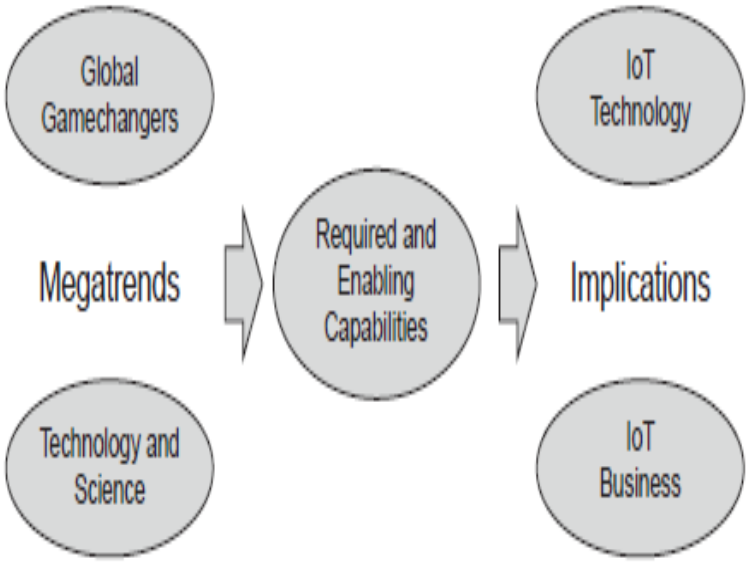
Examples : It includes applications like urban agriculture, robots and food safety tracing.

- **Urban Agriculture.**
  - Sensors and actuators can monitor and control the plant environment and tailor the conditions according to the needs of the specific specimen.

- Weather and light can be monitored, and necessary blinds that can shield and protect, as well as create greenhouse microclimates, can be automatically controlled.

➢ **Robots**

- The process chain of the mine involving blasting, crushing, grinding, and ore processing will be highly automated and interconnected.
- The heavy machinery used will be remotely controlled and monitored, mine sites will be connected, and shafts monitored in terms of air and gases.
- Sensors and actuators to remotely control both the sites and the massive robots in terms of mining machines for drilling, haulage, and processing are the instruments to make this happen.



➢ **Food Safety.**

- Sensors will provide the necessary monitoring capabilities, and tags like radio frequency identification (RFID) will be used to identify the items so they can be tracked and traced throughout the supply chain.
- From the monitoring of farming conditions for plant and animal health, registration of the use of pesticides and animal food, the logistics chain to monitor environmental conditions as produce is being transported, and retailers handling of food _ all will be connected

---

2.3 M2M towards IoT - the global context

➢ A set of megatrends are combining to create needs and capabilities, which in turn produce a set of IoT Technology and Business Drivers.

- A megatrend is a pattern or trend that will have a fundamental and global impact on society at a macro level over several generations.

Game changers

- The game changers come from a set of social, economic, and environmental shifts.
- Some of the more globally significant **game changers below**, and their relationship to IoT:

1. Natural Resource Constraints.

-The use of IoT to increase yields, improve productivity, and decrease loss across global supply chains is therefore escalating.

2. Economic Shifts.

- The overall economy is in a state of flux as it moves from the post-industrial era to a digital economy.

-As technology becomes increasingly embedded and more tasks automated, countries need to manage this shift and ensure that M2M and IoT also create new jobs and industries

3.Changing Demographics.

-Many countries will need to deal with an aging population without increasing economic expenditure.

-As a result, IoT will need to be used, for example, to help provide assisted living and reduce costs in healthcare and emerging "wellcare" systems.

4.Socioeconomic Expectations.

-Lifestyle and convenience will be increasingly enabled by technology as the same disruption and efficiency practices evident in industries will be applied within people's lives and homes as well.

5.Climate Change and Environmental Impacts.

-Technology, including IoT, will need to be applied to aggressively reduce the impact of human activity on the earth's systems.

6.Safety and Security.

- Public safety and national security becomes more urgent as society becomes more advanced, but also more vulnerable. This has to do both with reducing fatalities and health as well as crime prevention, and different technologies can address a number of the issues at hand.

7.Urbanization.

-Urbanization creates an entirely new level of demands on city infrastructures in order to support increasing urban populations

- IoT technologies will play a central role in the optimization for citizens and enterprises within the urban realm, as well as providing increased support for decision-makers in cities.

General technology and scientific trends

- Material Science

-It has a large impact across a vast range of industries, from pharmaceutical and cosmetics to electronics. MicroElectroMechanical Systems (MEMS) can be used to build advanced micro-sized sensors like accelerometers and gyroscopes.

-New materials provide different methods to develop and manufacture a large range of different sensors and actuators, as well being used in applications for environmental control, water purification, etc.

- Complex and Advanced Machinery

  -It refers to tools that are autonomous or semi-autonomous. Today they are used in a number of different industries; for example, robots and very advanced machinery is used in different harsh environments, such as deep-sea exploration, or in the mining industry in solutions such as Rio Tinto's Mine of the Future.

- Energy Production and Storage

  -It relates to the global interest of securing the availability of electricity while reducing climate and environmental impacts.

  -Smart Grids, for example, imply micro-generation of electricity using affordable photovoltaic panels. In addition, smart grids also require new types of energy storage, both for the grid itself and for emerging technologies such as Electric Vehicles (EVs) that rely on increasingly efficient battery technologies.

  -Wireless Sensor Networks (WSNs) will increasingly rely on different energy harvesting technologies and also rely on new miniaturized battery technologies and ultra capacitors.

Trends in information and communications technologies

- Sensors, actuators, and tags function as the digital interfaces to the physical world.

  -Tags using technologies such as RFID provide the means to put electronic identities on any object, and can be cheaply produced.

- Embedded processing is evolving,

  -not only towards higher capabilities and processing speeds, but also extending towards the smallest of applications.

- Instant access to the Internet is available

  -rapid deployment of cellular 3G and 4G or Long Term Evolution (LTE) systems on a global scale.

  -These systems provide ubiquitous and relatively cheap connectivity with the right characteristics for many applications, including low latency and the capacity to handle large amounts of data with high reliability.

- Software architectures

  -software development techniques from what were originally closed environments towards platforms.

- Web paradigm and using a service-oriented approach (SOA)

-By extending the web paradigm to IoT devices, they can become a natural component of building any application and facilitate an easy integration of IoT device services
into any enterprise system that is based on the SOA.

- Open APIs
  -Open APIs permit the creation of a fluid industrial platform, allowing components to be combined together in multiple different ways by multiple developers with little to no
  interaction with those who developed the platform, or installed the devices.
- Cloud computing
  It is one of the greatest aspects of the evolution of ICT for IoT as it allows virtualized and independent execution environments for multiple applications to reside in isolation on the same hardware platform, and usually in large data centers.
- Data processing and intelligent software
  -It will have an increasing role to play in IoT solutions.
- Big data
  -It refers to the increasing number and size of data sets that are available for companies and individuals to collect and perform analysis on.
- Decision support or even decision-making systems
  -It become very important in different application domains for IoT, as will the set of tools required to process data, aggregate information, and create knowledge.

Capabilities

- IoT systems are multimodal in terms of sensing and control, complex in management, and distributed across large geographical areas.
- For example, the new requirements on Smart Grids involve end-to-end management of energy production, distribution, and consumption, taking into consideration needs from Demand Response, micro-generation, energy storage, and load balancing.
- Industrialized agriculture involving automated irrigation, fertilization, and climate control is another example.
- Smart City solutions is a clear need for integration of multiple disparate infrastructures such as utilities, including district heating and cooling, water, waste, and energy, as well as transportation
  such as road and rail.
- Advanced remotely operated machinery, such as drilling equipment in mines or deep sea exploration vessels, will require real-time control of complex operations, including various degrees of autonomous control systems.
- IoT will allow more assets of enterprises and organizations to be connected, thus allowing a tighter and more prompt integration of the assets into business processes and expert systems.

- Simple machines can be used in a more controlled and intelligent manner, often called "Smart Objects."
- EVs are enabled by the new battery and energy storage technologies, but also require three separate elements to be connected _ cars, road infrastructure via charging poles, and the electricity grid. In addition, there are new charging requirements that are created by the use of EVs that need new means for billing, and in turn placing new requirements on the electricity grid itself.
- share information and services across organizations in the horizontal dimension, as well as being
  able to aggregate and combine services and information to reach higher degrees of refinement and values in the vertical dimension.
- ICT solutions to monitor and control assets, physical properties of the real world require not just increased levels of cyber security, but what can be referred to as cyber-physical security.
- In an IoT, where it is possible to control assets (e.g. vehicles or moveable bridges), severe amage to property, or even loss of life, is possible.

Implications for IoT

- In the M2M device area, there is an emerging consolidation of technologies where solutions across different industry segments traditionally rely on legacy and proprietary technologies.
- One example being Building and Home Automation and Control with legacy technologies like BACnet, Lonworks, KNX, Z-Wave, and ZigBee.
- Requirement for integration across multiple infrastructures and of a large set of different devices, as well as data and information sharing across multiple domains, there is a clear benefit from a horizontal systems approach with at least a common conceptual interoperability made available, and a reduced set of technologies and protocols being used.
- M2M is point problem-oriented, resulting in point solutions where devices and applications are highly dedicated to solving a single task.
- M2M devices are for this reason many times highly application-specific, and reuse of devices beyond the M2M application is possible.
- It allows easy integration in SOAs and attracts a larger application developer community.
- Both devices and connectivity have become viable for many different applications, and M2M today is centered on devices and connectivity.

Barriers and concerns

Concerns

- The first concern is the compromise of **privacy and the protection of personal integrity**. The use of RFID tags for tracing people is a raised concern

- Massive deployment of sensors in various environments, including in smartphones, explicit data and information about people can be collected, and using analytics tools, users could potentially be profiled and identified even from anonymized data.
- The reliability and accuracy of data and information when relying on a large number of data sources that can come from different providers that are beyond one's own control is another concern.
- the topic of **security** has one added dimension or level of concern.

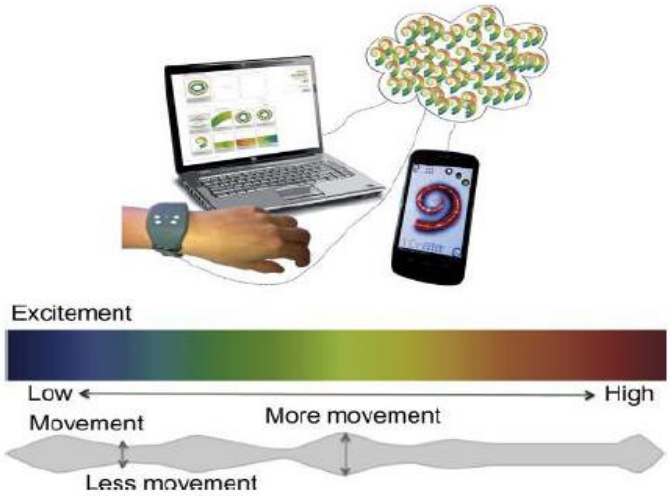
Barrier

- A perceived barrier for large-scale adoption of IoT is in costs for massive deployment of IoT devices and embedded technologies.
- From a technical perspective, what is desired is a high degree of automated provisioning towards zero-configuration

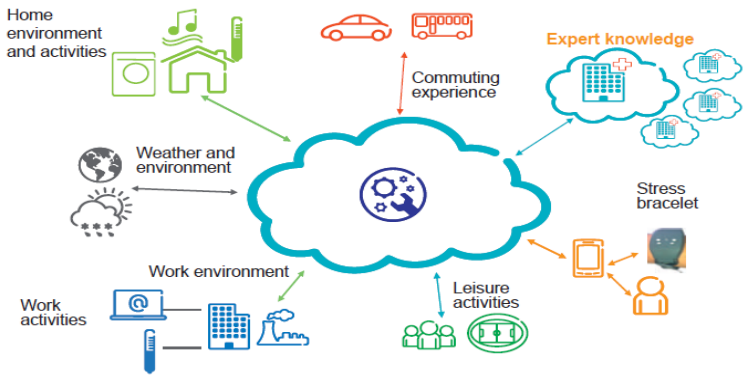
---

2.4 A use case example

- Studies from the U.S. Department of Health and Human Services have shown that close to 50% of the health risks of the enterprise workforce are stress related, which includes a group of factors such risks as high cholesterol, overweight issues, and high alcohol consumption
- As stress can be a root cause for many direct negative health condition.
- Measuring human stress can be done using sensors. Two common stress measurements are heart rate and galvanic skin response (GSR), and there are products on the market in the form of bracelets that can do such measurements.
- These sensors can only provide the intensity of the heart rate and GSR, and do not provide an answer to the cause of the intensity.
- The typical M2M solution would be based on getting sensor input from the person by bracelet.
- Using a smartphone as a mobile gateway to send measurements to an application server hosted by a health service provider.
- The application server hosts the necessary functionality to analyze the collected data, and based on experience and domain knowledge, provides an indication of the stress level.
- The stress information can then be made available to the person or a caregiver via smartphone application or a web interface on a computer.
- Stress measurement M2M solution is as follows

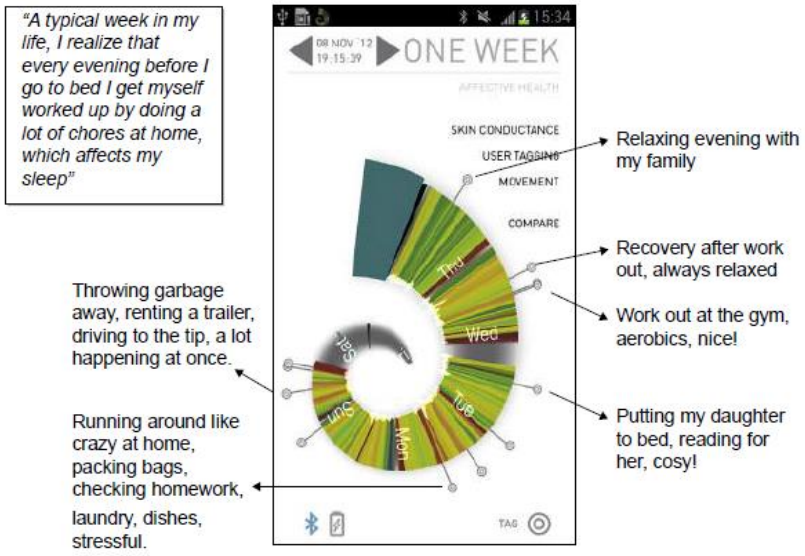


- Same problem situation from an IoT perspective would be to add data that provide much deeper and richer information of the person's contextual situation.
- The prospect is that the more data is available, the more data can be analyzed and correlated in order to find patterns and dependencies.
- Depicted is also the importance of having expert domain knowledge that can mine the available information, and that can also provide proposed actions to avoid stressful situations or environments.
- IoT-oriented stress analysis solution is as follows

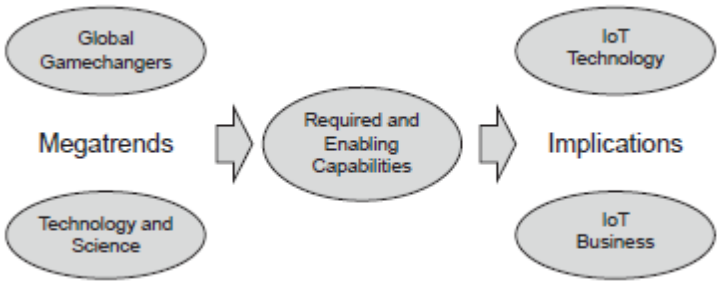


- smartphone application that provides stress analysis feedback.

- an IoT-oriented solution t



o solving a particular problem could provide much more precision in achieving the desired results.

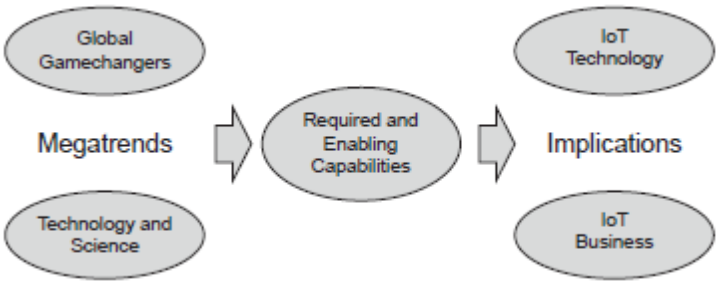


2.5 Differing characteristics

Characteristics of M2M

- It is generally focused on solving a problem at a particular point for one company or stakeholder.
- It does not typically take a broad perspective on solving a larger set of issues
- most M2M devices are special purpose devices that are application-specific

- M2M solutions are therefore also vertical siloes with no horizontal integration or connection



to adjacent use cases

- M2M applications are built by very specialized developers, and deployed inside enterprises.
- M2M is also very device- and communication-centric

A Comparison of the Main Characteristics of M2M and IoT

M2M	**IoT**
M2M is about direct communication between machines	IoT is about sensor automation and internet platform
It supports point to point communication	It supports cloud communication
Devices do not necessarily rely on an internet connection	Devices rely on an internet connection
It is mostly hardware based technology	It is both hardware and software based technology
Machine normally communicate with a single machine at a time	Many users can access at one time over the internet
A device can connected through mobile or other network	Data delivery depends on the Internet Protocol Network

Aspect	M2M	IoT
Applications and services	Point problem driven	Innovation driven
	Single application - single device	Multiple applications - multiple devices
	Communication and device centric	Information and service centric
	Asset management driven	Data and information driven
Business	Closed business operations	Open market place
	Business objective driven	Participatory community driven
	B2B	B2B, B2C
	Established value chains	Emerging ecosystems
	Consultancy and Systems Integration enabled	Open Web and as-a-Service enabled
	In-house deployment	Cloud deployment
Technology	Vertical system solution approach	Horizontal enabler approach
	Specialized device solutions	Generic commodity devices
	De facto and proprietary	Standards and open source
	Specific closed data formats and service descriptions	Open APIs and data specifications
	Closed specialized software development	Open software development
	SOA enterprise integration	Open APIs and web development

.....

A Market Perspective

2.6 Introduction

- The increasing interest in M2M and IoT solutions has been driven by the potential large market and growth opportunities.
- In M2M and IoT, the technology used for these solutions may be very similar , even use the same base components but the data is managed will be different.
- In an M2M solution, data remains within strict boundaries ,it is used solely for the purpose.
- In IoT, data may be used and reused for many different purposes.
- Data can be shared between companies and value chains in internal information marketplaces.
- Data could be publicly exchanged on a public information marketplace.
- A Marketplace Perspective is as follows

UNIT-4

2

Elements of Internet of Things Security

2.1 Introduction

IoT is a novel paradigm which is becoming popular in research community and industry due to its wide range of applications. The fundamental idea is that IoT will connect all objects around us to provide seamless communication and contextual services offered by them. Economics of scale in the IoT presents new security challenges for ubiquitous devices in terms of authentication, addressing and embedded security. Devices like RFID and sensor nodes most often have no access control functionality and can freely obtain information from each other. As a result, an authentication as well as authorization scheme must be established between these devices to achieve the security goals for IoT. Without any strong security, IoT malfunctions and attacks will overweigh of its benefits. Privacy of things and security of data is one of the key challenges in the IoT. Security will become more serious issue as the IoT becomes an integral part of everyday life. The numbers of embedded systems like refrigerator, washing machines to TV are connected to the Internet, but the vast majority of these systems are un-patchable, or poorly maintained.

Pervasive and ubiquitous nature of IoT makes a set of new challenges beyond merely making the systems work, and prominently amongst the challenges is to provide improved security. This chapter presents requirements and challenges for handling successful security in IoT. In this chapter threat modeling, threat analysis and use cases and misuse cases are also discussed.

2.1.1 Vulnerabilities of IoT

General security needs and devices life cycle in the context of IoT for Building, Automation and Control (BAC) system are presented in [1]. In BAC system, there is a network of interconnected nodes that performs various functions like heating, ventilating and air conditioning. All nodes carries different functionality and maximum of these devices are resource

constrained like sensor nodes. Life of devices starts when they are manufactured to perform specific tasks and hence there are devices from different manufacturers. Due to this reason, trust bootstrapping and interoperability are major issues. Next phase is installation and commissioning within IoT network based on device identity and secret keys. Procedures for installation and bootstrapping are defined for fix period of time. After this, device become operational and runs the functions of BAC system. During operational phase, devices are under the control of resource owner and occasional maintenance is required. Maintenance includes software up-gradation and reconfiguration. Due to operational changes on devices, they may require re-bootstrap. The device continues for the operational phase and the eventual maintenance phase until the device is decommissioned at the end of its lifecycle. Figure 2.1 shows the generic lifecycle of a thing. This generic lifecycle is also applicable for the IoT scenarios other than BAC systems.

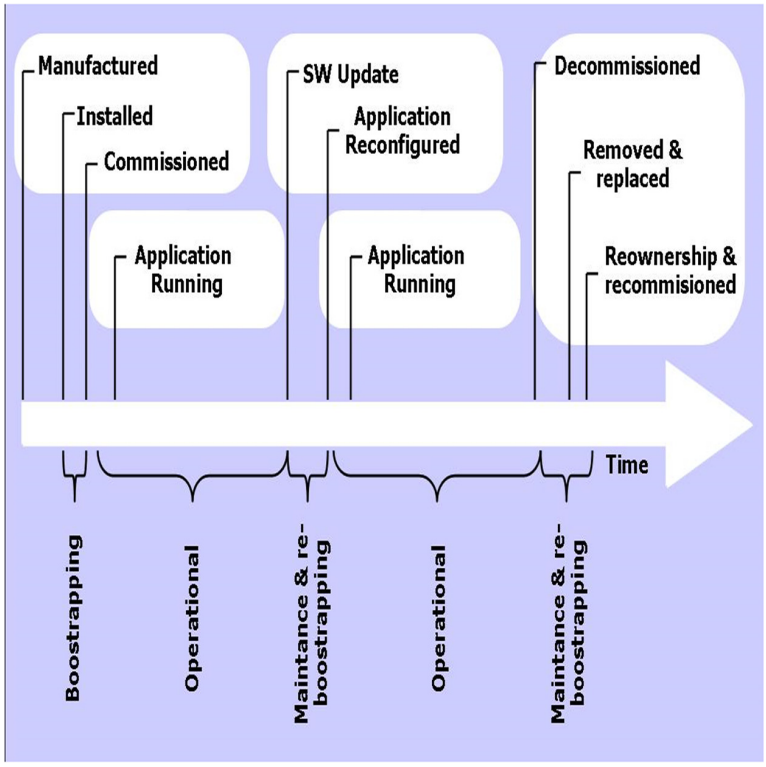


Figure 2.1 The life cycle of a device in IoT [1]

Life cycle of devices shows that, there are many vulnerabilities and security relationship between devices and secure interaction need to be addressed. In the IoT context, security is not limited to the required security services, but should be also extended to overall system and functionalities. Vulnerabilities are fact of life in IoT and information security. Dynamic network topology and, distributed nature makes IoT more vulnerable to security threats, and attacks. Mobility and weak physical security of low power devices in IoT networks are also possible causes for security vulnerabilities. Attacks are grouped into two types: passive attacks and active attacks. In passive attacks, attackers are interested in eavesdropping and monitoring of data transmission. In other words, attacker does not attempt to perform modifications. Active attacks can be in the form of modification, fabrication and interruption. Denial of service (DoS) attacks is one of the example active attacks. Threats include identity theft through masquerading or spoofing, unauthorized access to resources, unauthorized disclosure or modification of data. IoT opens your home to cyber threats. With reference to device life cycle in the IoT, Figure 2.2 depicts vulnerabilities of IoT. Possible vulnerabilities of IoT are as follows:

1. **Unauthorized access:** One of the main threats is the tampering of resources by unauthorized access. These access rights may be granted to

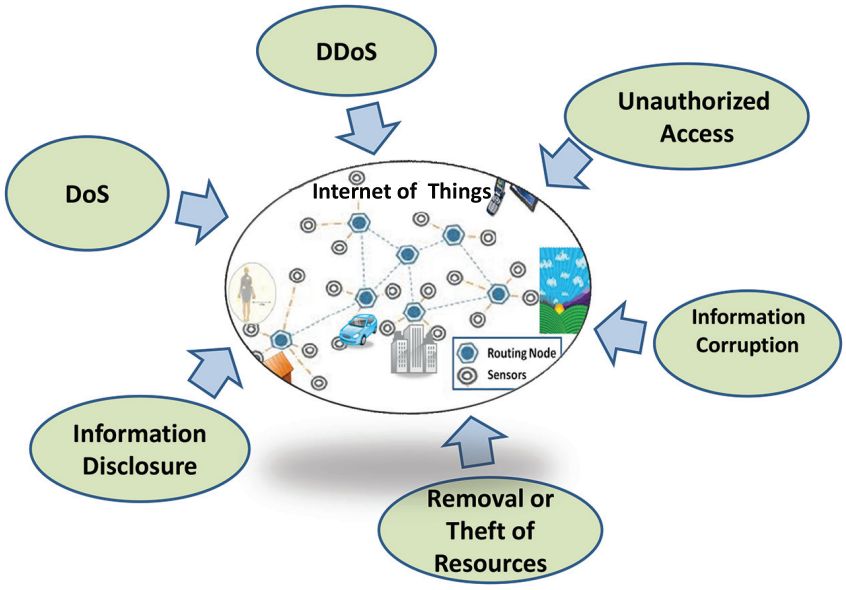


Figure 2.2 Vulnerabilities of IoT

an unauthorized entity if an attacker is able to get hold of the authorization process. Identity-based verification should be done before granting the access rights.

2. **Information corruption:** Other threat is information corruption and, to address this, the device credentials must be protected from tampering. Secure design of access rights, credential and, exchange is required to avoid corruption.
3. **Theft of resources:** The access of shared resources over insecure channel causes theft of resources, or data flow, and results into man-in-the-middle attack.
4. **Information disclosure:** In IoT, the data is stored at different places in different forms depending on the context. This distributed data must be protected from disclosure. The context-aware access control must be enforced to regulate access to system resources.
5. **DoS attack:** A DoS attack makes an attempt to prevent legitimate user from accessing services which they are eligible for [2]. For example unauthorized user sends to many requests to server so as to flood the network and deny other legitimate users from access to the network.
6. **DDoS:** Distributed Denial of Service (DDoS) is a type of DoS attack where multiple compromised systems – which are usually infected with a Trojan – are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack [3].

   CyberBunker Launches "World's Largest" DDoS Attack, Slows down the Entire Internet. A massive cyberattack launched by the Dutch web hosting company CyberBunker has caused global disruption of the web, slowing down internet speeds for millions of users across the world, according to a BBC report. CyberBunker launched an all-out assault, described by the BBC as the world's biggest ever cyberattack, on the self-appointed spam-fighting company Spamhaus, which maintains a blacklist used by email providers to filter out spam [4].

Here are few real examples of attacks that hit the IoT [5].

1. First there was the Carna Botnet. At its peak, 420,000 'things,' such as routers, modems, printers were compromised.

2. Then TRENDnet's connected cameras were hacked, with feeds from those cameras published online, forcing the FTC to make its first ever IoT judgement.
3. Another is the Linux.Darlloz – PoC IoT worm found in the wild by Symantec, while most recently Proofpoint discovered a Botnet of 100,000 compromised systems including connected things such as TVs, routers and even a fridge.

2.1.2 Security Requirements

IoT security requirements to counter the threats like tampering, fabrication and theft of resources are listed below:

1. ***Access control***
   The access control provides authorized access to network resources. IoT is ad-hoc, and dynamic in nature. Efficient and a robust mechanism of secure access to resources must be deployed with distributed nature.
2. ***Authentication***
   Authentication is an identity establishment between communicating parties (devices). Due to diversity of devices, and end users, there should be an attack resistant and lightweight solution for authentication.
3. ***Data confidentiality***
   Data confidentiality is protecting data from unauthorized disclosure and data tampering. Secure, lightweight, and efficient key exchange mechanism is required due to dynamic network topology.
4. ***Availability***
   Availability is ensuring no denial of authorized access to network resources. Access control and availability problems are critical due to the wireless nature of ad-hoc networks.
5. ***Trust management***
   Trust management, and trust-based access control are basic requirements in IoT due to its nomadic nature. Decision rules needs to be evolved for trust management in IoT.
6. ***Secure software execution***
   It refers to a secure, managed-code, runtime environment designed to protect against deviant applications.

7. ***Secure storage***
   Secure storage involves confidentiality and integrity of sensitive information stored in the system.
8. ***Tamper resistance***
   It refers to the desire to maintain these security requirements even when the device falls into the hands of malicious parties, and can be physically or logically probed.
9. ***Scalability***
   IoT system will consist of various types of devices in terms of different capabilities (from intelligent sensors and actuators, to home appliances) as well communication means (wire or wireless) and protocols (Bluetooth, ZigBee, RFID, Wi-Fi, etc), and across different geographical locations. As a result, the system is highly distributed, heterogeneous, and pervasive. Dealing with such type of system, scalability is an important point in designing a security solution.
10. ***Flexibility and adaptability***
    IoT will likely to consist of mobile communication devices which can roam around freely from one type of environment to the others with different type of risks and security threats. Furthermore, users are likely to have different privacy profile depending on environment or with whom they are communicating. Therefore, flexibility and adaptability are the other important requirements for a security solution in IoT.

Figure 2.3 depicts high level security architecture for IoT with possible threats, and attacks. This architecture provides systematic way of countering the above threats. Right side of the architecture shows possible threats in IoT. Threats include destruction of resources by unauthorized access, information disclosure, information corruption, theft of resources, and information disclosure. Security dimensions shown in this architecture are the mitigation principles to counter these threats.

As explained and presented in the Figure 2.3, main security requirements/ objectives in IoT includes access control, authentication, confidentiality, availability and the trust management.

2.1.3 Challenges for Secure Internet of Things

IoT is an intelligent collaboration of tiny sensors and devices giving new challenges to security and privacy in end-to-end communication of things. Protection of data and privacy of things is one of the key challenges in the IoT [6].

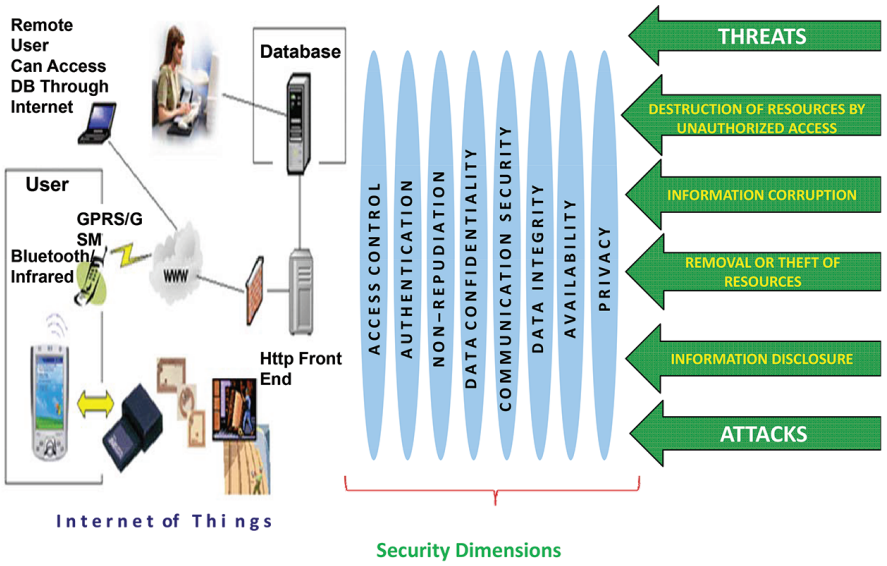


Figure 2.3 Security architecture for IoT

Security challenges identified in the IoT context are as follows:

1. **Identity management (IdM) for devices**
   - New Identity concepts, and their implications in IoT world
   - Identity delegation, imprinting of identity in things, merging identities to create a meta-identity, etc.
   - Trust Management, Circles of Trust (IoT belonging to different owners)
   - Identity and privacy
   - Authentication schemes for IoT
   - Secure attribute exchange, and selective disclosure of attributes inside IoT
2. **Secure interactions in/with IoT**
   - Secure, and certified context information for things
   - Reliable computation, and storage services provided by IoT
   - Interaction of things in a Better-Than-Nothing Security (BTNS) environment
   - Secure, and dynamic network, and space composition, discovery, namespace, resolution and indexing of things
   - Auditing of interactions with things
   - Physical and virtual mobility of things

3. **Distributed access control and privacy**
    - Dynamic exchange of authenticated identity information between things
    - Credential Management, and bootstrapping with single sign on for things
    - Privacy-aware policy-based authorization systems with deductive policies, and delegation
    - Dynamic selection of applicable policies based on the environment in IoT
    - Dynamic attributes negotiation for things
    - Proxy security services with delegation for things, in particular, for 6LowPAN devices privacy-aware negotiation, and application of attribute releasing policies
4. **Secure data management and exchange**
    - Assurance for the information exchange between things
    - Secure, and private management of distributed data spread across multiple things
    - Personal data auditing, and enhanced audit data visualization for users to make them understand the usage of their identities, and data by things
    - Signed context information for exchange with things controlled by user privacy policies
    - Secure storage, and deletion of audit data in a distributed IoT environment
5. **End-to-End security**
    - End-to-end security measures between IoT devices and Internet hosts are equally important.
    - Applying cryptographic schemes for encryption and authentication codes to a packet is not sufficient for the resource constrained IoT.
    - Hence future research is required into efficient end-to-end security measures between IoT and the Internet [7].
6. **Privacy**
    - Privacy is one of the most sensitive areas in the context of IoT.
    - In IoT, all objects are connected to the Internet and they communicate with each other over the Internet. Hence the privacy issue is crucial.

- As the Internet gets expanded with new types of devices and heterogeneous networks, IoT users and devices have to access the digital world with wide range of protocols and methods.
- Further, as ownership of these devices by the users does not exist, the issue of privacy is getting more serious [7].

7. **Security structure**
   The IoT will remain stable-persisting as a whole over time. In the sequel, putting together the security mechanism of each logical layer cannot implement the defense-in-depth of system [8]. So it is a challenging and important research area to construct security structure with the combination of control and information [9]. Challenges presented above shows that, there is a need of integrated approach of authentication, and access control for ubiquitous devices in IoT. Furthermore, the solution for authentication and access control must be attack resistant from the well-known attacks.

2.2 Threat Modeling

Threat modeling is presented by first defining misuse case i.e. negative scenario describing the ways the system should not work and then standard use case. The assets to be protected in IoT will vary with respect to every scenario case. The modeling of the security attacks helps to understand an actual view of the IoT networks and enable us to decide the mitigation plans [7].

2.2.1 Threat Analysis

We recommend that the assets needs to be identified to drive threat analysis process and also to guide specification for security requirements. Let's consider the smart home example which is subset of IoT. Smart home is localized in space, provide services in a household. Devices in the Smart Home are federated into a network and furnish means for entertainment, monitoring of appliances, controlling of house components and other services. In the scenario of trusted smart home service, data assets would include data stored on the end user device, data typed by the user, the data stored in database or data transmitted over communication medium (E.g. location data). Also passkey which authorizes owner to access home must be protected from unauthorized access and its integrity should be maintained as well as authentication needs to be taken care. These assets are expected to be the main targets of a malicious

attack. Devices or users are granted access rights to protected resources and services. These rights are implemented as credentials which must be safeguarded by an attacker. Detail use case and misuse case for smart home system is described in Section 2.2.2.

2.2.2 Use Cases and Misuse Cases

The actor in use case and misuse case in the scenario of smart home includes: Infrastructure owner (smart home), IoT entity (smartphone device or software agent), attacker (misuser) and intruder (exploiter).

- Access control

This operations deal with issuing access rights to protected resources and systems. Granting of voting credentials, passkey issuance and granting of access rights are few examples.

In Table 2.1, use case and misuse case clearly depicts how the smart home is prone to attack for access control operations. There are several use cases possible for different scenario cases. In the sequel, different threats collected and control objectives are summarized below:

a) Access rights granted to unauthorized entity

Access rights may be granted to an unauthorized actor if an attacker is able to subvert the access control process. One way to do this may be done through impersonation, social engineering, by sending targeted e-mails requesting for access rights etc.

Table 2.1 Use case and misuse case for access control

Use Case		**Misuse Case**	
Granting Access		Access Rights Granted to Unauthorized Device	
Description	Actor gets access to resource	Description	Misuser granted access rights directly
Precondition	Actor has access privilege	Precondition	Actor has sufficient privilege to perform this operation
Success flow	Actor confirms identity of requesting actor Credential verification Granting of access	Assumption	Misuser is able to impersonate a legitimate access requesting entity
Actor	Infrastructure owner/ requesting device	Actor	Misuser
		Assets	Access credentials

1. Access rights should only be granted to actors after verification of their identity.
2. Provision of filters or other equivalent mechanism should be installed to identify type of actors.
3. If no formal verification of identity possible, then there should be alert provision before granting access rights.

b) Corruption of access credentials

Depending on the chosen solution used for representing access right credentials, attacker is able to get hold of certain options. If the credentials are stored with the device they may be subject to manipulation by a malicious entity (user / device). This can be used to gain extra privileges by tampering with the credential's data structure.

1. A secure design should be used to implement credential storage. Credentials should be stored on a device or should be generated depending on the context, to avoid tampering by an attacker.
2. Otherwise integrity of credentials should be protected by cryptographic means.

c) Unauthorized data transmission

Unauthorized data sent by an entity of an IoT network may lead to a breach of privacy. Even the number or the different types of devices constitute private data, measures to be followed are as follows:

1. Traffic monitoring should be detected
2. Integrity of messages should be taken care

d) Denial of service (DoS) attack

If a successful DoS attack can be mounted against the smart door software agent or then notification alerts about the door open status can be suppressed. If this attack is combined with the first one then access to the Smart Home can be obtained.

1. Software agent should be proofed against tampering and DoS attacks.

e) Man-in-the-middle attack

Federation over insecure network may lead to eavesdropping which may be exploited further for data theft or identity theft.

1. Federation requests should only be accepted from entities after verification of their identity.
2. Strong encryption techniques should be employed to protect confidentiality of identity or location to ensure identity/location privacy.

A threat analysis presented may also comprise a risk analysis where severity and probability can be estimated and then risk can calculated for each threat. The objective of this use case and misuse case-based threat modeling is to incorporate them in the security assessment of IoT networks.

2.2.3 Activity Modeling and Threats

The activity modeling of IoT attacks is use to understand the sequence of actions taking place when the attacks are happening. When there is solution for authentication and IdM, its needs to be analyzed for adversary models. Adversaries have been defined in many ways [10, 11] in literature. If we know, and understand possible attacks, we can decide countermeasures, and mitigation to deal with those attacks [12]. Security threats are designed using attack tree where root node represents attack goal, leaf nodes represents different ways of achieving the goals, and internal nodes represents attack steps. Discovery and avoidance of threats, and attacks in the system or networks is the most important task. To this purpose, we can use attack modeling like a graph-based collaborative attack modeling [13] in which sample of attack scenarios are used to demonstrate the attack steps.

Privacy model is required for privacy protection against adversaries. Adversary is someone whose purpose is opposed to, or conflict with the system functionality. Adversary is classified based on their capabilities like nature as active, or passive, static, or adaptive, computational ability, mobility, and byzantine. Adversary models are subject to change depending on the underline application [14]. Adversaries are classified based on their capacities into three types as [14]:

1. ***Weak passive:*** These are passive eavesdropper with limited capacity, and cannot gain whole control over transmission path.
2. ***Strong passive:*** These are passive eavesdropper, and can gain whole control over transmission path.
3. ***Strong active:*** These are active eavesdropper with the ability of compromising intermediate source, and destination.

In the view of these adversaries, as shown in Figure 2.4, IoT is prone to man-in-the-middle attack, impersonation which can cause DoS attack, and replay attack. In IoT, any device can communicate with any other device through wireless media, or through Internet. Possible communications are between device-to-device, human-to-device, human-to-human giving connection between heterogeneous entities, or network. Figure 2.4 presents general use case of IoT where MobileEntity(x): A mobile device represents an entity i.e. any device in the network which communicates with other entities of the same type, or of different types via Internet, or direct. Mobile Entity 1, 2, 3 represent three different and most probable scenarios in the system

Figure 2.4 IoT use case [7]

of communication. Different possible attacks in IoT communications are described below.

- ***Man-in-the-middle attack***

When the devices are commissioned into a network, keying material, security, and domain parameters could be eavesdropped. Keying material can reveal secret key between devices and authenticity of the communication channel could be compromised. Man-in-the-middle attack is one type of eavesdropping possible in commissioning phase of devices to IoT. Key establishment protocol is vulnerable to man-in-the-middle attack and compromise device authentication as devices usually do not have prior knowledge about each other. As device authentication involves exchange of device identities, identity theft is possible due to man-in-the-middle attack. A sample of man-in-the-middle attack is shown in Figure 2.5.

- ***DoS attack***

All the devices in IoT have low memory, and limited computation resources, thus they are vulnerable to resource enervation attack. Attackers can send messages, or requests to a specific device so as to consume their resources. This attack is more daunting in IoT as the attacker might be single, and resource constrained devices are large in numbers. DoS attack is also possible due to man-in-the-middle attack. A sample of DoS attack in IoT scenario is shown in Figure 2.5.

- ***Replay attack***

While exchange of identity related information or other credentials in IoT, this information can be spoofed, altered or replayed to repel network traffic. This causes a very serious replay attack. Replay attack is essentially one form of active man-in-the-middle attack. Replay attack can be prevented by maintaining the freshness of random numbers, for example by using time stamp or nonce by including Message Authentication Code (MAC) as well. Sample of replay attack is shown in Figure 2.5.

To this purpose, authentication, and access control are the main security issues which are to be addressed. As per the adversary model presented, a strong active type of adversary which is most powerful needs to compromise the proposed authentication scheme.

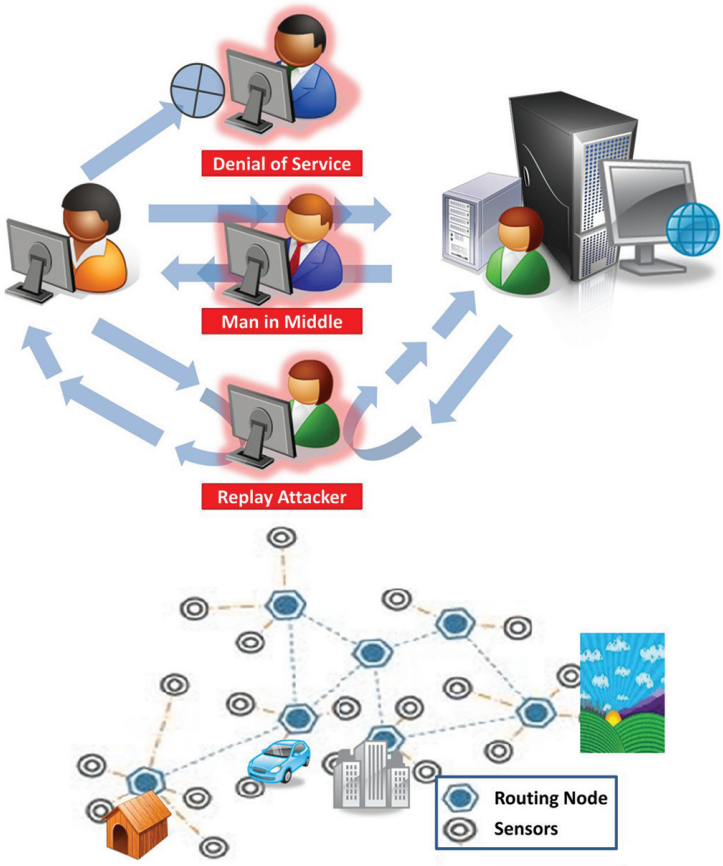


Figure 2.5 IoT attacks scenario [7]

2.2.4 IoT Security Tomography

As presented in [15], this section presents security tomography in the IoT context. It is classified according to attacks addressing to different layers. Here we have considered layers namely transport layer, network layer, MAC layer and RF layer. Figure 2.6 illustrates the IoT security tomography and the layered attacker model.

I) Threats on transport layer

Depending on types of protocol used in transport layer attacks are classified. By interfering connection of connection based protocol (E.g. TCP) can be

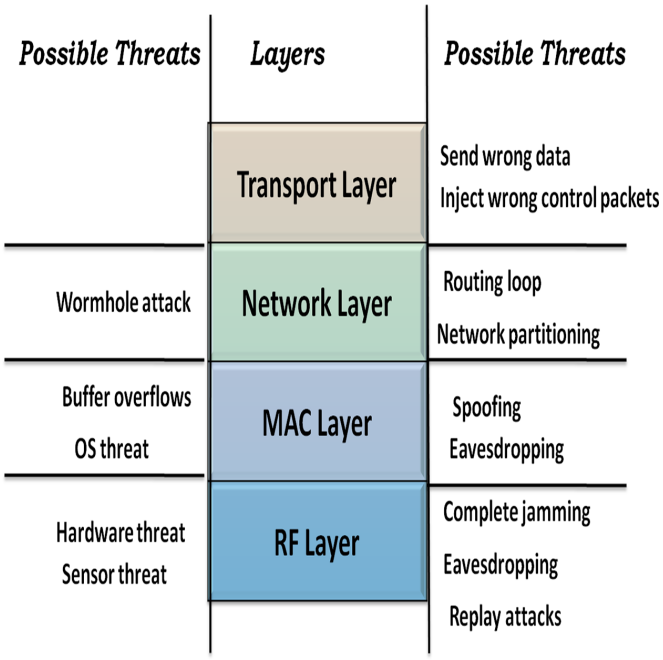


Figure 2.6 IoT security tomography and layered attacker model

tampered. Connectionless protocols like UDP usually do not have sequence or session number and also do not provide error and flow control. That is why packets are getting in incorrect order or some packets can also be lost. Threats possible on transport layer are as follows:

1. **Send wrong data:** Sending of packets with wrong information enforces error correction on the receiver node, which requires CPU power and therefore results into additional energy consumption.
2. **Inject wrong control packets:** Injection of packets into a running connection can enforce to close, de-sync or interfere the connection [15]. The packet injection process allows an unknown third party to disrupt or intercept packets from the consenting parties that are communicating, which can lead to degradation or blockage of users' ability to utilize certain network services or protocols [16].

II) Threats on network layer

Attacker in the network layer intends at disturbing and degrading the routing service. Threats on network layer are as follows:

1. **Routing loop:** The attacker simply forges new routing packets or modifies existing ones to create cyclic packet trajectory. These packets cyclically traverse nodes and they never reach their destination. This type of attack shortens network lifetime by consuming valuable network resources [15].
2. **Network partitioning:** This type of attack has the most serious impact on the overall routing service. The adversary separates the network to disjoint set of nodes that cannot reach each other. It can be achieved by injecting falsified routing packets or simply by other interventions that cause some nodes, which are cut-set nodes the removal of which cause the network to partitioned, to be break down sooner because of energy depletion [15].
3. **Wormhole:** The wormhole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended wormhole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. It either drops or selectively forwards the packets, leading to network disruption. [17].

   A wormhole attack is caused by one, two or more number of nodes. In one ended wormhole, fake neighbors are created by establishing high power node. Two ended wormhole is the most commonly found type of wormhole. It can be set via an out-of-band channel between two nodes or by encapsulating packet. In the latter case the nodes on way from first wormhole end to other, cannot increment hop count and thus wormhole attack becomes the result [18].

III) Threats on MAC layer

Attacks to the medium access layer are based on the shared medium characteristic of the broadcast medium. More precisely, the focus on security threats of this category arises from point-to-point local broadcast over a shared medium. Possible threats on MAC layer are as follows:

1. **Spoofing:** Unauthorized parties may participate in the network, e.g. by spoofing their identities and using the identity of another device.
2. **Eavesdropping:** Eavesdropping by nature is possible on a broadcast medium. An attacker who is physically located within the transmission range of the sender device receives all the traffic and can read it unless there is no protection mechanism in place

IV) Threats on RF layer

Attacks on the radio can be subdivided into jamming, spying and replay.

1. **Complete jamming:** Due to increasing level of noise level, the communication becomes difficult and eventually impossible anymore. For example the communication of a group of sensors can be disabled in order to avoid propagation of alarm triggering information [15]
2. **Eavesdropping:** Broadcasted RF-information can be received. It is an initial step of gathering transmitted information.
3. **Replay attacks:** Recorded RF-information can be replayed at wrong time even without knowing the content of the packets. It confuses the receiver or can set it into wrong state.

Different threats like sensor threat, hardware threats and OS threats are also possible in IoT.

I) OS threat: Attacks on the OS can be categorized in attacks that want to change the behavior of the nodes and in attacks that want to disable the node or a critical service of the OS. Attacks that change the behavior of the node can be categorized into attacks that can be done remotely and attacks that require direct contact to the hardware [15].

1. **Buffer overflows:** Such attacks intentionally force a buffer to store more data than it is intended to hold. The overflowed data can alter binary code and therefore the behavior of the node.
2. **Direct reprogramming:** Sensor nodes that can be directly accessed (collected) can be manually reprogrammed by changing applications, OS, OS services that are stored in RAM or ROM.

II) Hardware threat: Here attacks are classified by direct electrical access to the internal components of the device, e.g.: micro-probing.

III) Sensor threat: Such attacks are classified by a direct electrical access to the internal components of the device, for example by micro-probing. This attack is also called as falsified sensor reading [15].

2.3 Key Elements

Threats are potential causes of an event that could breach security and causes possible harms. Some time there is situation where protection mechanism becomes subject to harm. To avoid these, some security policies are decided. Threats are occur due to weaknesses in the mechanism which implementing a particular security policy.

Security in IoT environment should address the following main issues [19].

- Enabling smart and intelligent behavior of networked objects.
- Preservation of privacy for heterogeneous sets of objects.
- Decentralized authentication and trust model.
- Energy efficient security solutions.
- Proper authentication of the objects within the network.
- Security and trust for cloud computing services.
- Data ownership.

Key elements of security are,

1. Authentication (Identity establishment) which can set up proof of identities;
2. Access Control specifies who can access;
3. Data and message security are referred as data integrity and confidentiality;
4. Prevention from denial of taking part in a transaction, whether as an initiating or a receiving party, known as non-repudiation [20] and availability states that resources or information should be accessible to authoritative party at all instant.

Further details of the elements of system security are explained in following points.

2.3.1 Identity Establishment

As mentioned above, secure entity identification is known as identity establishment which is also referred as authentication. Authentication is an identity establishment between communicating parties (devices) or entities. Entity can be a single user, a set of users, an entire organization or some networking device. Identity establishment is ensuring that the origin of an electronic document and message is correctly identified. Identities are the windows through which users interact with their devices, and consume services in today's world. Before any service is delivered, it is customary to verify a digital identity of the user requesting that service (user identity) and also the identity of the entity offering the service (service identity). In IoT world, this concept of identity extends to things. Ensuring that things have a means to be identified is critical to assure users that their interactions with things are safe.

Many security mechanisms have been proposed based on private key cryptographic primitives due to fast computation and energy efficiency.

Scalability problem and memory requirement to store keys makes it inefficient for heterogeneous devices in IoT. A public key cryptography based solution overcomes these challenges because of its high scalability, low memory requirements and no requirement of key pre-distribution infrastructure [7].

In [21], the author presented ECC based mutual authentication protocol for IoT using hash functions. Mutual authentication is achieved between terminal node and platform using secret key cryptosystem introducing the problem of key management and storage. Self-certified keys cryptosystem based distributed user authentication scheme for WSN is presented in [22], where only user nodes are authenticated

2.3.2 Access Control

Access control is also known as access authorization or simply authorization. The principles of access control determine who should be able to access what [2]. Access control prevents unauthorized use of resources. To achieve access control, entity which trying to gain access must be authenticated first. According to authentication, access rights can be modified to the individual. Introducing a new device, or user, and achieving authentication and access control to devices resources in IoT is critical. As IoT is ad-hoc, and dynamic in nature, efficient, and a robust mechanism of secure access to resources must be deployed with distributed nature. Traditionally, access control is represented by an Access Control Matrix (ACM), in which the column of ACM is basically a list of objects, or resources to be accessed and the row is a list of subject or whoever wants to access the resource. From this ACM, two traditional access control models exist, i.e. Access Control List (ACL) and capability-based access control. Due to unbound number of devices, and services, scalability, and manageability issues are daunting in IoT. Various access control models and their applicability in the context of IoT is presented and discuss in detail in chapter 6 of this book.

2.3.3 Data and Message Security

Data security is mostly concerned with source authenticity, modification detection, and confidentiality of data that is being processed in-memory, or while residing on a storage medium or during transmission over a computer network. Combination of modification and confidentiality of message is not enough for data integrity, but origin of authenticity is also important. Location privacy is equally important risk in IoT. To ensure location privacy, communication and reference signal integrity needs to be maintained.

Communication confidentiality and privacy of localization and tracking data is highly sensitive in IoT amalgam. There should not be any way for an attacker to reveal identity or location information of device to ensure privacy. When the contents of message are changed after sending this message from source but before reaches at destination then we can say that integrity of message is lost. Integrity services assure that data sent are received as no duplication, insertion, modification, or replays.

2.3.4 Non-repudiation and Availability

Non-repudiation (NR) is one of the security services (or dimensions as defined in the document X.805 by the ITU) for point-to-point communications [23]. Non-repudiation of action is the process by which an entity (sender or receiver) is prevented from denying a transmitted message. So when message is sent, receiver can prove that initiating sender only sent that message. Similarly sender can prove that receiver got the message. To repudiate means to deny. For many years, authorities have required to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so [24].

Both X.800 and RFC 2828 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system i.e., a system is available if it provides services according to the system design whenever users request them. For example banking customers should be able to check their balance at any time so server must be available at all time.

Availability is ensured by strictly maintaining all hardware, repairing immediately whenever require. It also prevents the bottleneck occurrence by keeping emergence backup power systems and guarding against malicious actions like Denial of Service (DoS) attack.

2.3.5 Security Model for IoT

Integrated and interrelated perspective on security, trust, privacy can potentially deliver an input to address protection issues in the IoT [6]. Therefore cube structure is chosen as a modeling mechanism for security, trust and privacy. A cube has three dimensions with the ability to clearly show the intersection thereof. Therefore a cube is an ideal modeling structure

for depicting the convergence of security, trust and privacy for the IoT. In IoT access information, required to grant/reject access requests, is not only complex but also composite in nature. This is a direct result of the high level of interconnectedness between things, services and people. It is clear that the type and structure of information required to grant/reject such an access request is complex and should address the following IoT issues: security (authorization), trust (reputation), privacy (respondent). This is depicted in Figure 2.7.

Current Internet security protocols rely on a well-known and widely trusted suite of cryptographic algorithms: the Advanced Encryption Standard (AES) block cipher for confidentiality; the Rivest-Shamir-Adelman (RSA) asymmetric algorithm for digital signatures and key transport; the Diffie-Hellman (DH) asymmetric key agreement algorithm; and the SHA-1 and SHA-256 secure hash algorithms. This suite of algorithms is supplemented by

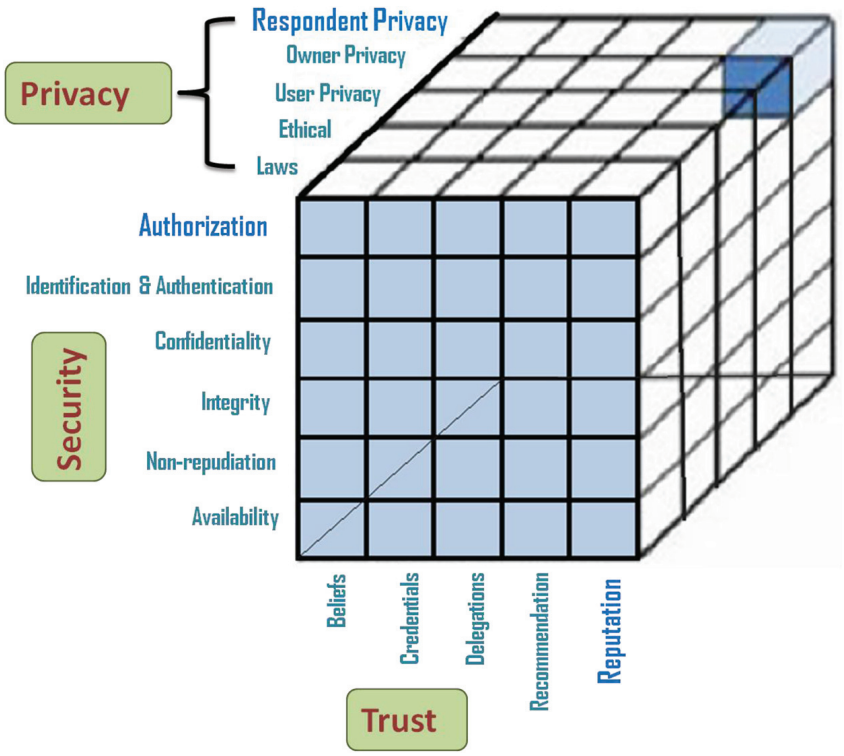


Figure 2.7 Security model for IoT

a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC). Adoption of the ECC algorithms has been slowed by significant IPR concerns, but publication of RFC 6090 and recent IPR disclosures may encourage adoption [25].

2.4 Conclusions

In the environment of IoT interactions between devices, user and service provider should be secure, in spite of the type of devices used to access a service. We must assure that enough privacy and security is available before the technology gets deployed and becomes a part of our daily life. A lightweight, distributed and attack resistant solution are the most vital properties for the security solution in IoT. This puts resilient challenges for IdM and access control of devices. The access control is very important for successful realization of IoT, especially due to the dynamic network topology, and distributed nature.

The incremental deployment of the technologies that will make up the IoT must not fail what the Internet has failed to do: provide adequate security and privacy mechanisms from the start. We must be sure that adequate security and privacy is available before the technology gets deployed and becomes part of our daily live. Security requirement and threat taxonomy insist to go for trusted platform module which offers facilities for the secure generation of cryptographic keys. Threat modeling, threat analysis and activity modeling of threats presented in this chapter are used to understand the sequence of different possible attacks, and accordingly it is easy to consider what action has to takes place when the attacks are happening. Identity establishment, access control, data and message security, non-repudiation and availability are the most vital elements which needs to be considered for the security in the IoT. This chapter also presents security model for the IoT with the convergence of trust and privacy.

Referneces

[1] T. Heer, O. Gracia-Morchon, R. Hummen, S.L. Koch, S. Kumar, and K. Wehrle, “Security challenges in the IP-based Internet of Things,” In wireless Personal Communications, 61(3): 527–542, 2011.
[2] Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill
[3] http://www.webopedia.com/TERM/D/DDoS_attack.html

UNIT-5

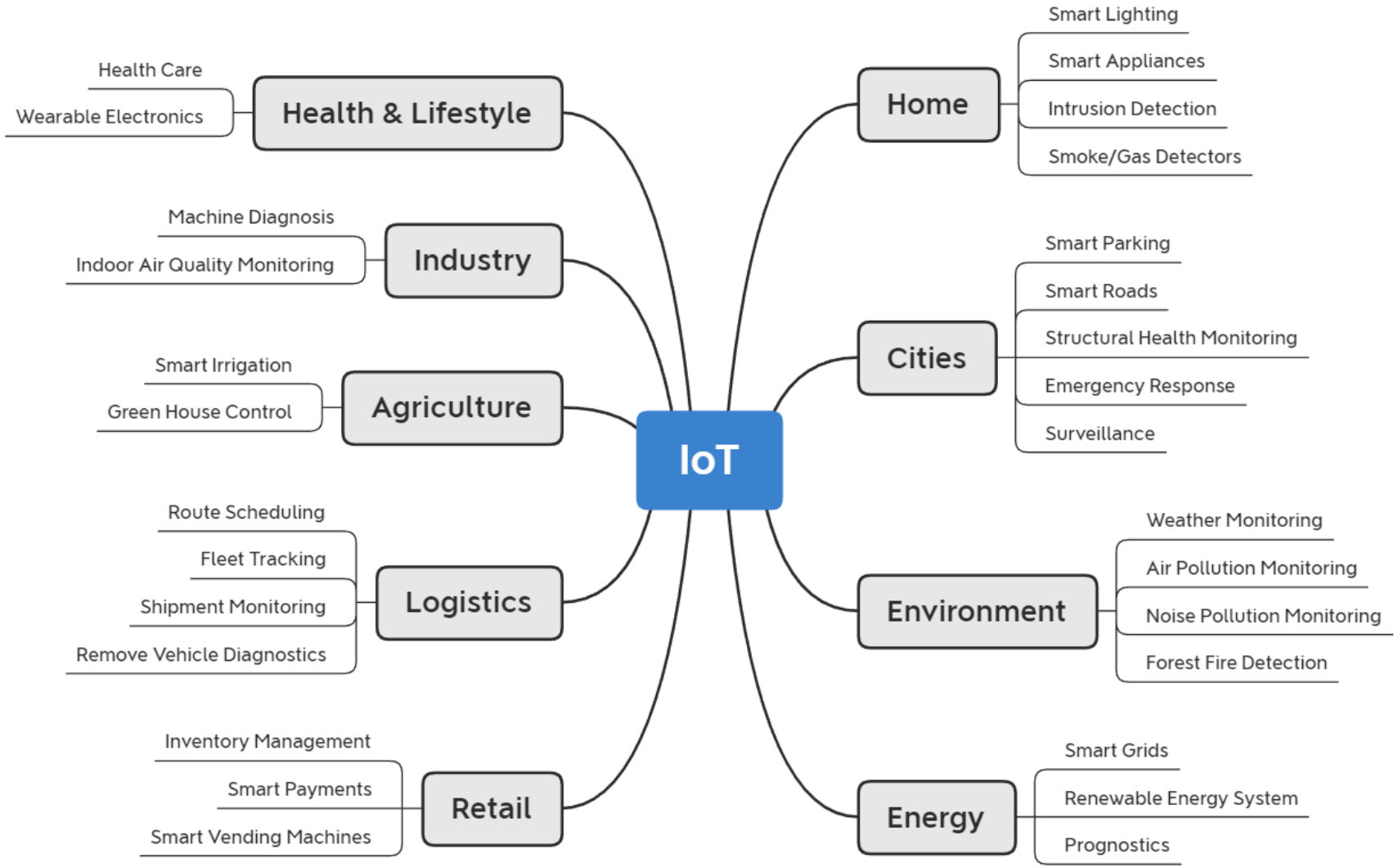
Chapter 2

Domain Specific IoTs

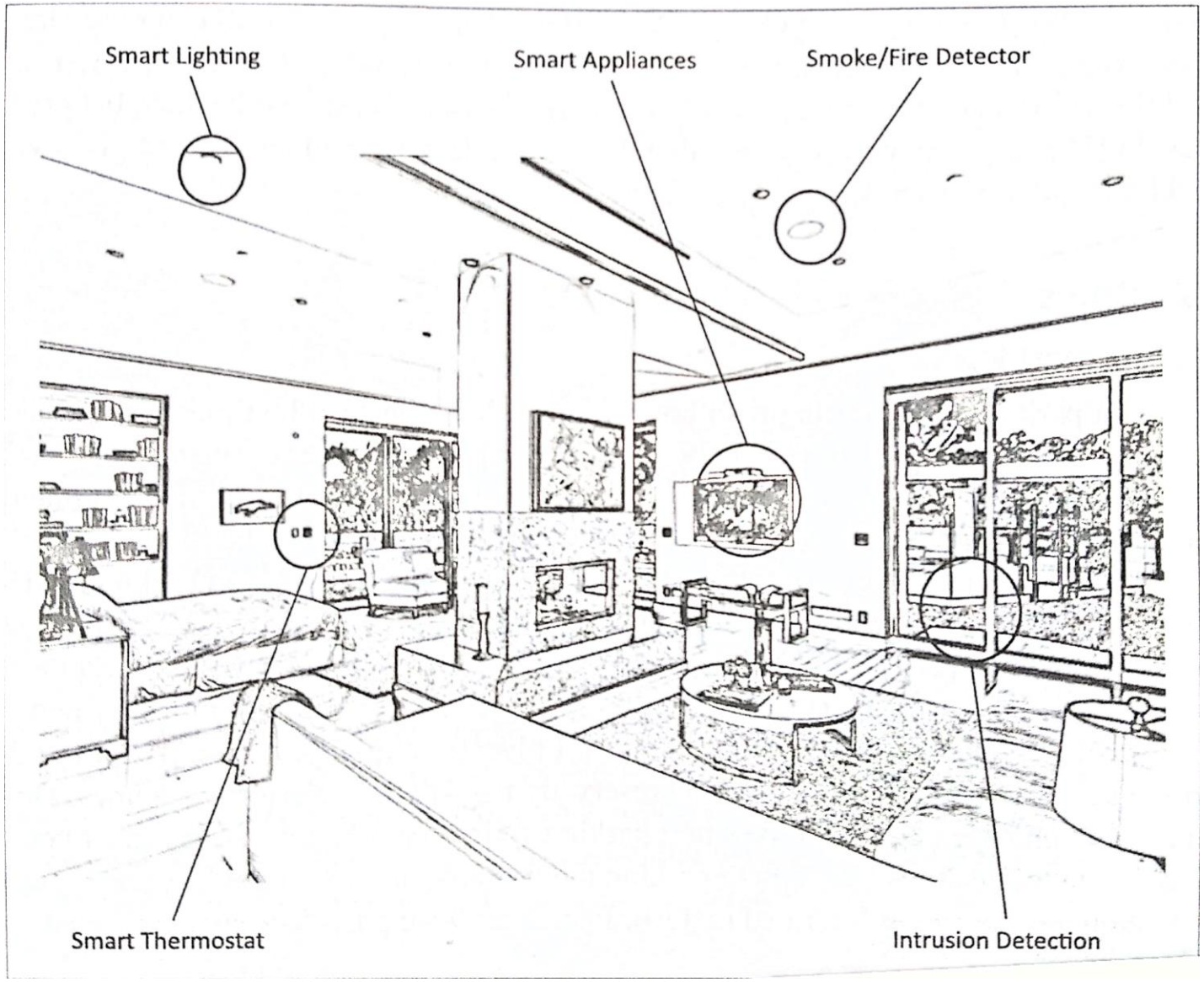
Outline

- Introduction
- Home Automation
- Cities
- Environment
- Energy
- Retail
- Logistics
- Agriculture
- Industry
- Health & Lifestyle

Introduction – Applications of IoT



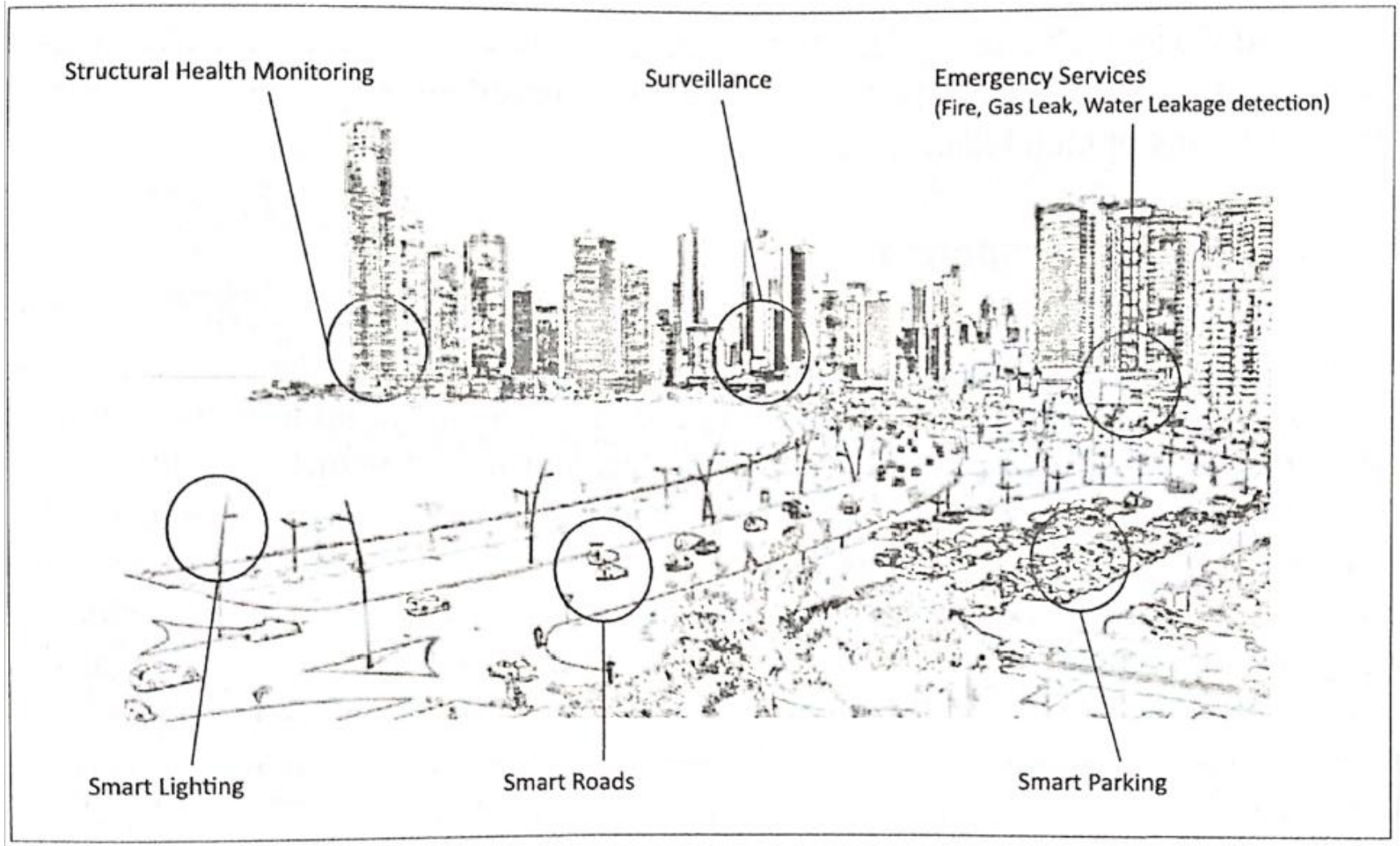
Home Automation



Home Automation (2/2)

- Smart Lighting
  - Control lighting by remotely (mobile or web applications)
- Smart Appliances
  - Provide status information to the users remotely
- Intrusion Detection
  - Use security cameras and sensors (PIR sensors and door sensors)
  - Detect intrusions and raise alerts
  - The alerts form: an SMS or an email sent to the user
- Smoke/Gas Detectors
  - Use optical detection, ionization, or air sampling techniques to detect the smoke
  - Gas detectors can detect harmful gases
    - Carbon monoxide (CO)
    - Liquid petroleum gas (LPG)
  - Raise alerts to the user or local fire safety department

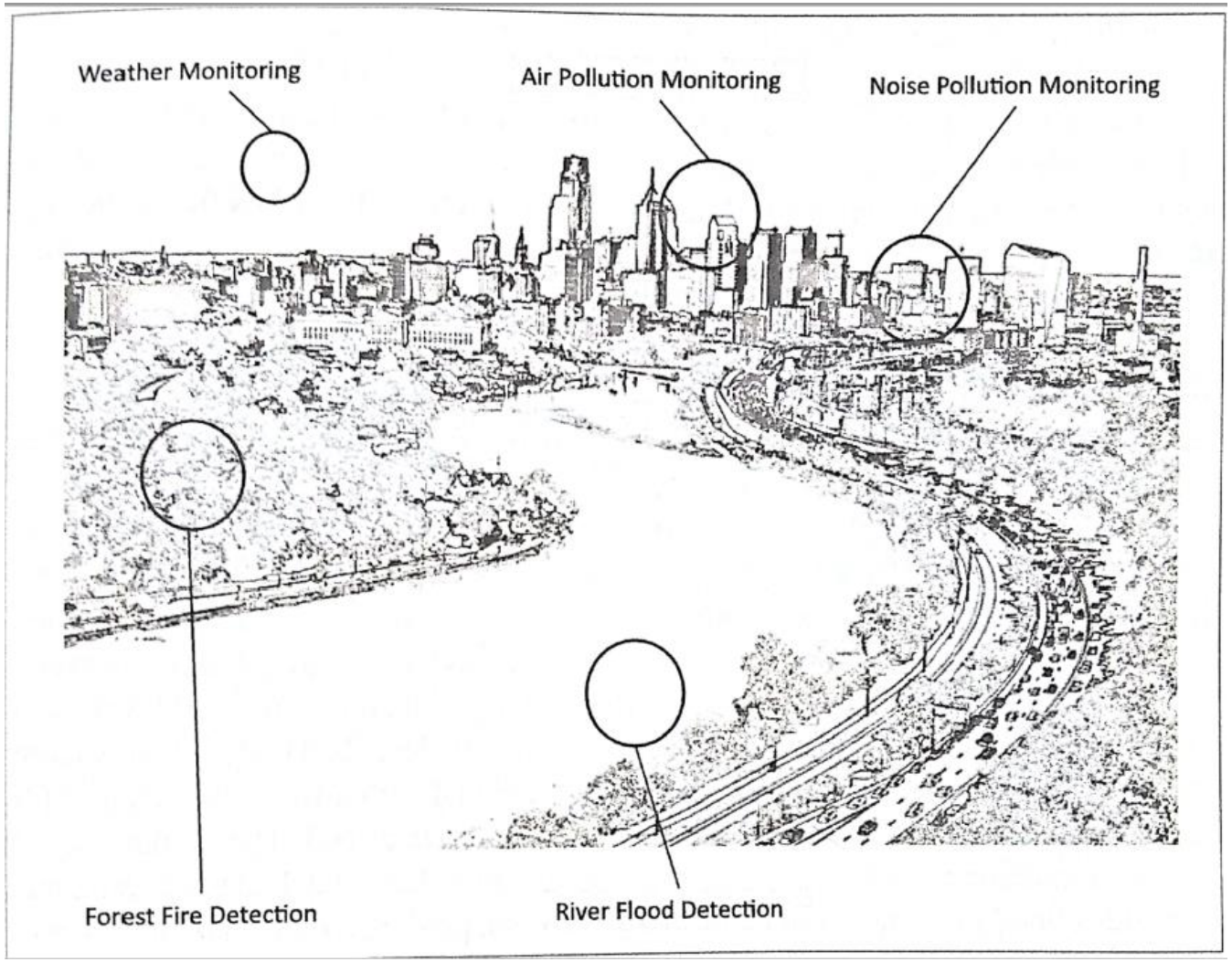
Cities (1/2)


Structural Health Monitoring
Surveillance
Emergency Services
(Fire, Gas Leak, Water Leakage detection)
Smart Lighting
Smart Roads
Smart Parking

Cities (2/2)

- Smart Parking
  - Detect the number of empty parking slots
  - Send the information over the internet and accessed by smartphones
- Smart Roads
  - Provide information on driving conditions, traffic congestions, accidents
  - Alert for poor driving conditions
- Structural Health Monitoring
  - Monitor the vibration levels in the structures (bridges and buildings)
  - Advance warning for imminent failure of the structure
- Surveillance
  - Use the large number of distributed and internet connected video surveillance cameras
  - Aggregate the video in cloud-based scalable storage solutions
- Emergency Response
  - Used for critical infrastructure monitoring
  - Detect adverse events

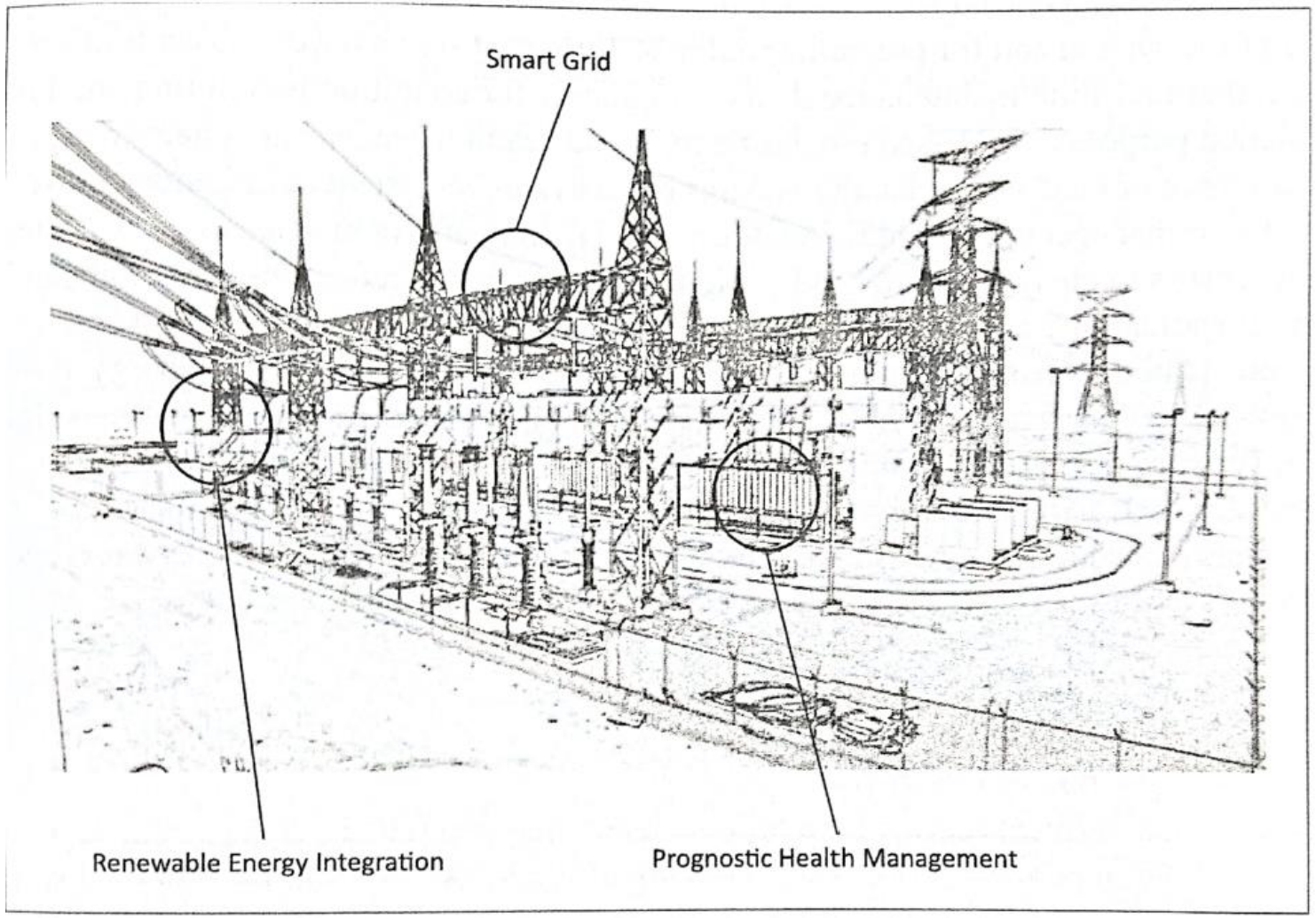
Environment (1/2)



Environment (2/2)

- Weather Monitoring
  - Collect data from several sensors (temperature, humidity, pressure, etc.)
  - Send the data to cloud-based applications and storage back-ends
- Air Pollution Monitoring
  - Monitor emission of harmful gases (CO_2, CO, NO, NO_2, etc.)
  - Factories and automobiles use gaseous and meteorological sensors
  - Integration with a single-chip microcontroller, several air pollution sensors, GPRS-modem, and a GPS module
- Noise Pollution Monitoring
  - Use a number of noise monitoring stations
  - Generate noise maps from data collected
- Forest Fire Detection
  - Use a number of monitoring nodes deployed at different locations in a forests
    - Use temperature, humidity, light levels, etc.
  - Provide early warning of potential forest fire
  - Estimates the scale and intensity
- River Floods Detection
  - Monitoring the water level (using ultrasonic sensors) and flow rate (using the flow velocity sensors)
  - Raise alerts when rapid increase in water level and flow rate is detected

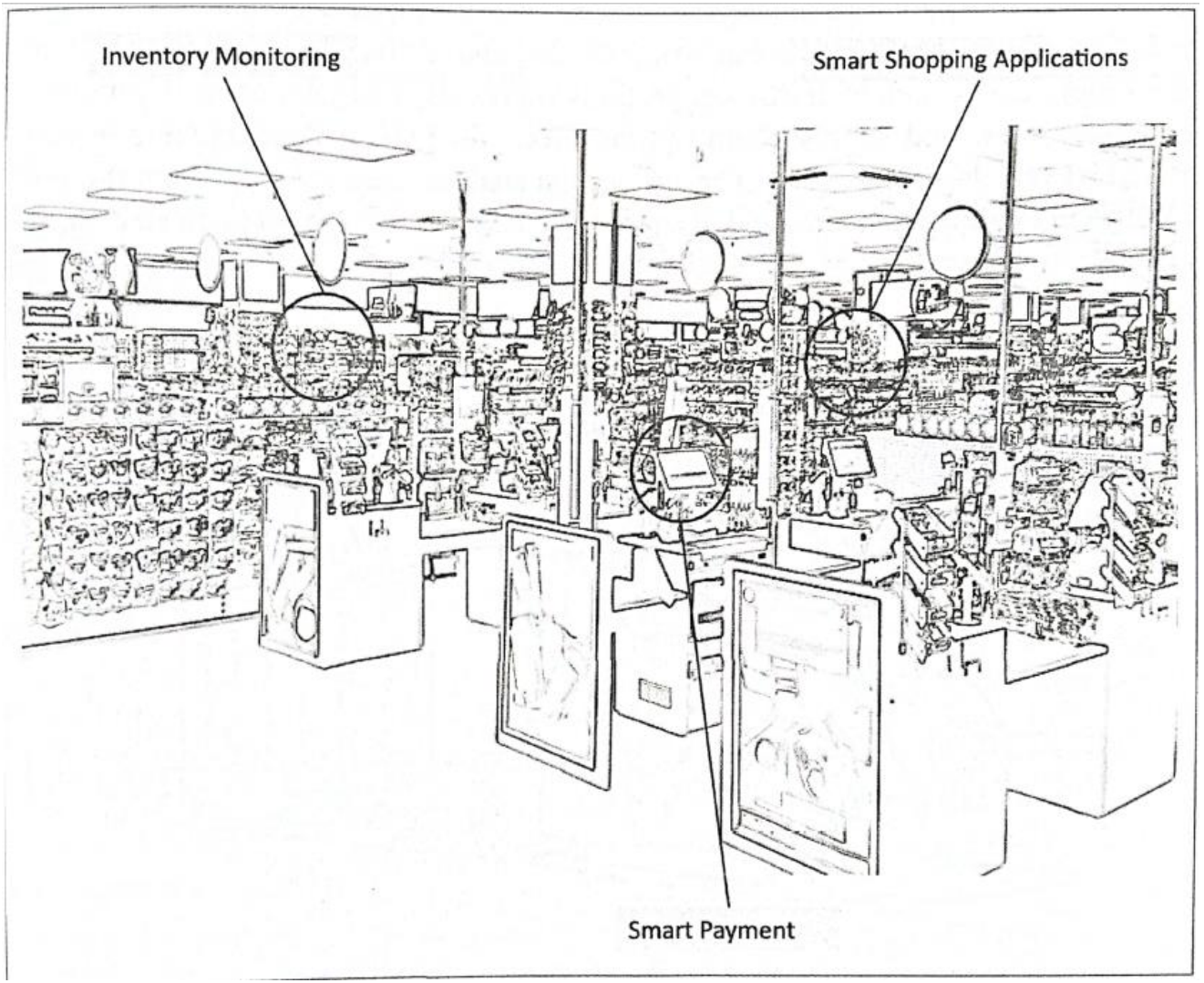
Energy (1/2)


Smart Grid
Renewable Energy Integration
Prognostic Health Management

Energy (2/2)

- Smart Grids
  - Collect data regarding electricity generation, consumption, storage (conversion of energy into other forms), distribution, equipment health data
  - Control the consumption of electricity
  - Remotely switch off supply
- Renewable Energy Systems
  - Measure the electrical variables
  - Measure how much the power is fed into the grid
- Prognostics
  - Predict performance of machines or energy systems
    - By collect and analyze the data from sensors

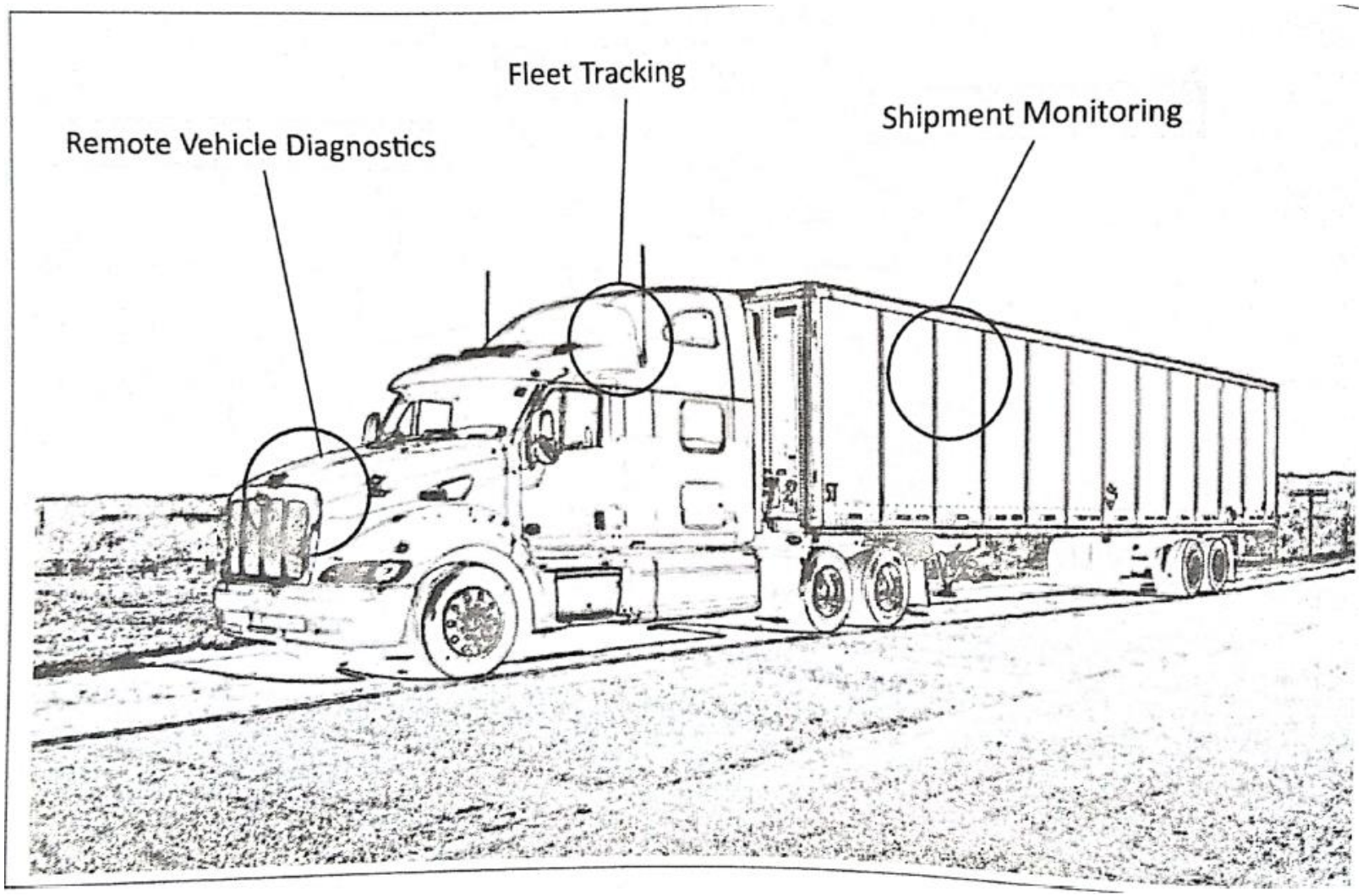
Retail (1/2)


Inventory Monitoring
Smart Shopping Applications
Smart Payment

Retail (2/2)

- Inventory Management
  - Monitoring the inventory by the RFID readers
  - Tracking the products
- Smart Payments
  - Use the NFC
    - Customers store the credit card information in their NFC-enabled
- Smart Vending Machines
  - Allow remote monitoring of inventory levels
  - Elastic pricing of products
  - Contact-less payment using NFC
  - Send the data to the cloud for predictive maintenance
    - The information of inventory levels
    - The information of the nearest machine in case a product goes out of stock in a machine

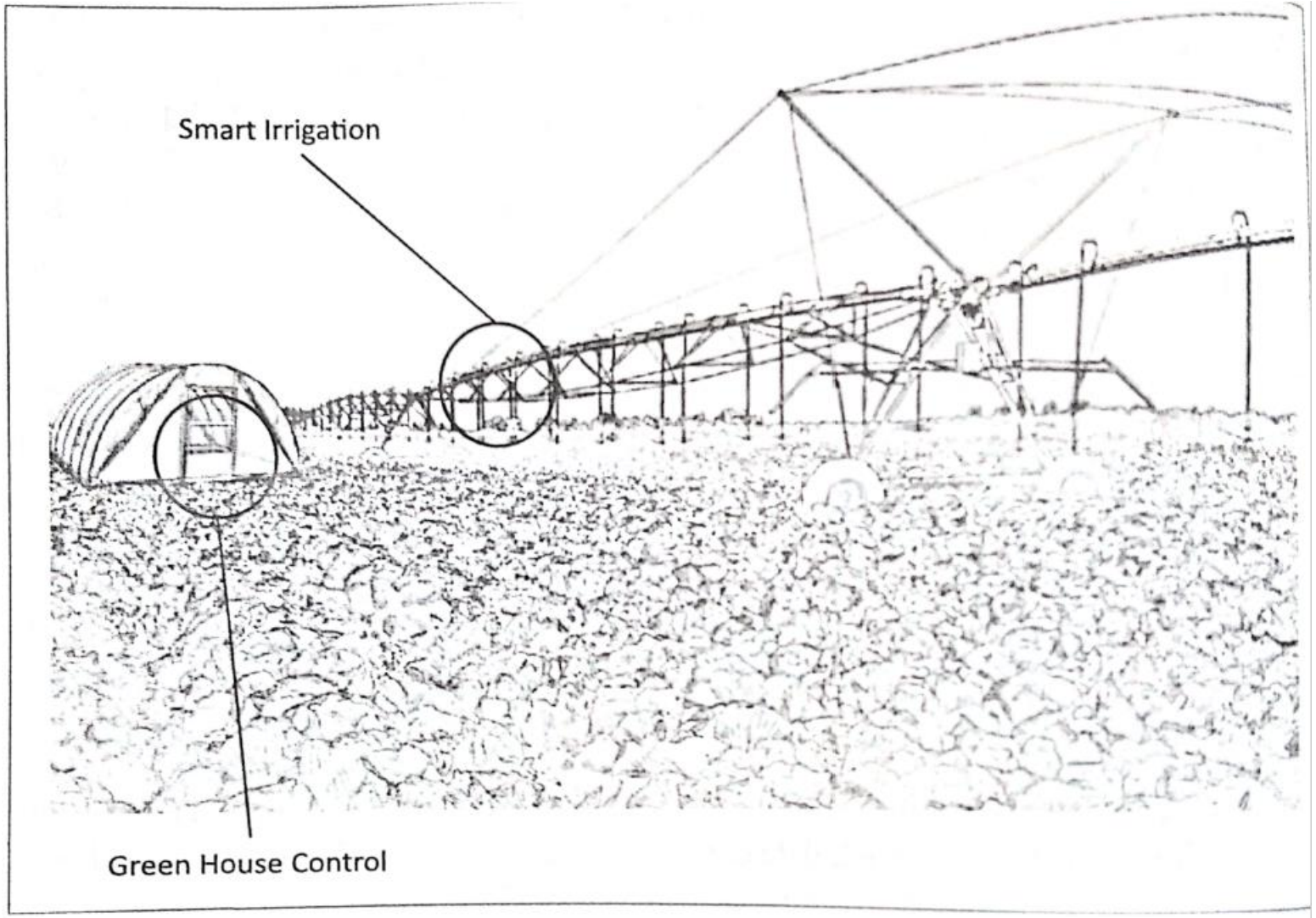
Logistics (1/2)



Logistics (2/2)

- Route Generation & Scheduling
  - Generate end-to-end routes using combination of route patterns
  - Provide route generation queries
  - Can be scale up to serve a large transportation network
- Fleet Tracking
  - Track the locations of the vehicles in real-time
  - Generate alerts for deviations in planned routes
- Shipment monitoring
  - Monitoring the conditions inside containers
  - Using sensors (temperature, pressure, humidity)
  - Detecting food spoilage
- Remote Vehicle Diagnostics
  - Detect faults in the vehicle
  - Warn of impending faults
  - IoT collects the data on vehicle (speed, engine RPM, coolant temperature)
  - Generate alerts and suggest remedial actions

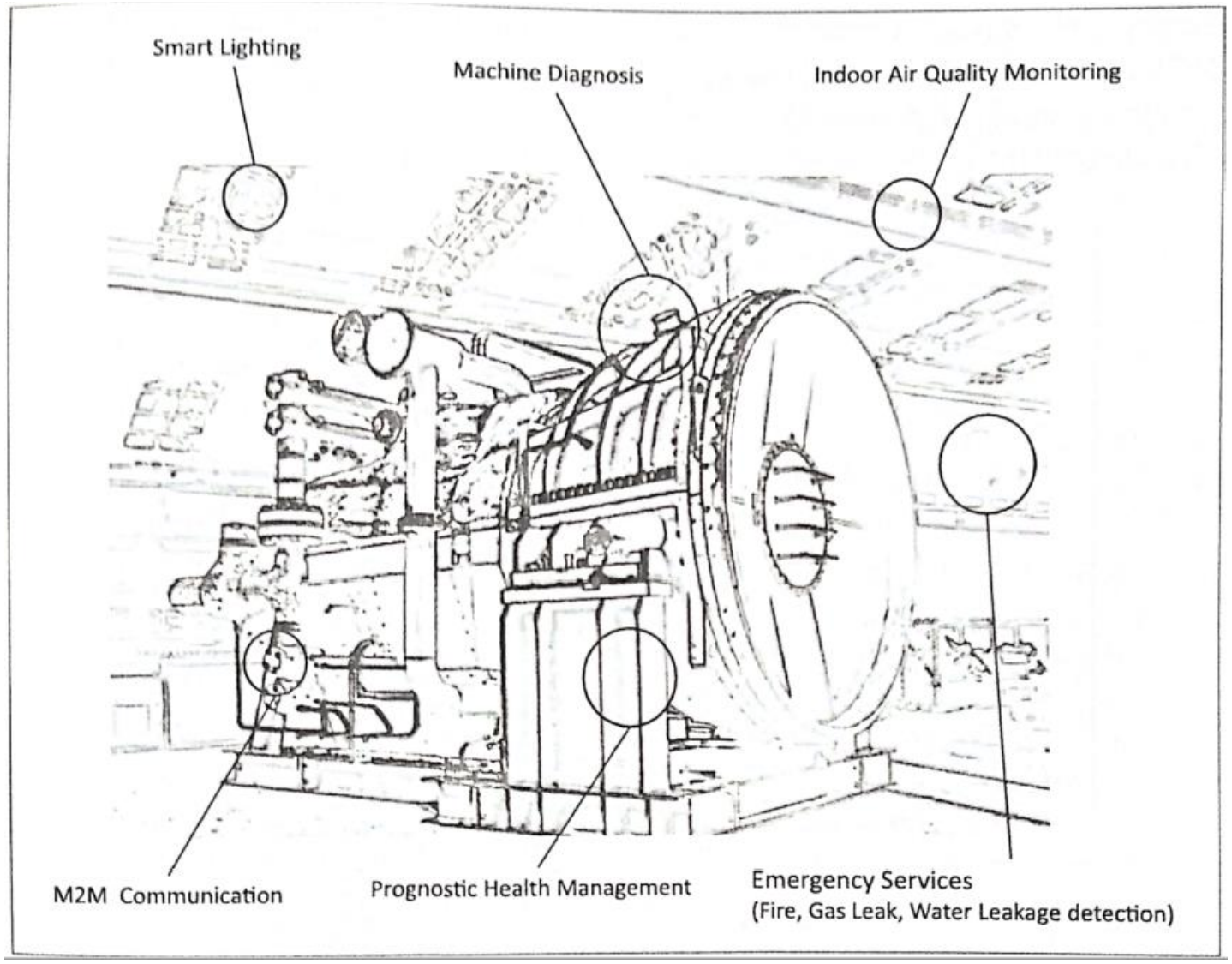
Agriculture (1/2)



Agriculture (2/2)

- Smart Irrigation
  - Use sensors to determine the amount of moisture in the soil
  - Release the flow of water
    - Using predefined moisture levels
  - Water Scheduling
- Green House Control
  - Automatically control the climatological conditions inside a green house
    - Using several sensors to monitor
    - Using actuation devices to control
      - Valves for releasing water and switches for controlling fans
  - Maintenance of agricultural production

Industry (1/2)


Smart Lighting
Machine Diagnosis
Indoor Air Quality Monitoring
M2M Communication
Prognostic Health Management
Emergency Services
(Fire, Gas Leak, Water Leakage detection)

Industry (2/2)

- Machine Diagnosis
  - Sensors in machine monitor the operating conditions
    - For example: temperature & vibration levels
  - Collecting and analyzing massive scale machine sensor data
    - For reliability analysis and fault prediction in machines
- Indoor Air Quality Monitoring
  - Use various gas sensors
    - To monitor the harmful and toxic gases (*CO*, *NO*, NO_2, etc.)
  - Measure the environmental parameters to determine the indoor air quality
    - Temperature, humidity, gaseous pollutants, aerosol

Health & Lifestyle

- Health & Fitness Monitoring
  - Collect the health-care data
    - Using some sensors: body temperature, heart rate, movement (with accelerometers), etc.
  - Various forms : belts and wrist-bands
- Wearable electronic
  - Assists the daily activities
    - Smart watch
    - Smart shoes
    - Smart wristbands

Internet of Things
A Hands-On Approach

Chapter 9:
Case Studies Illustrating IoT Design

Outline

- Smart Lighting
- Home Intrusion Detection
- Smart Parking
- Weather Monitoring System
- Weather Reporting Bot
- Air Pollution Monitoring
- Forest Fire Detection
- Smart Irrigation
- IoT Printer

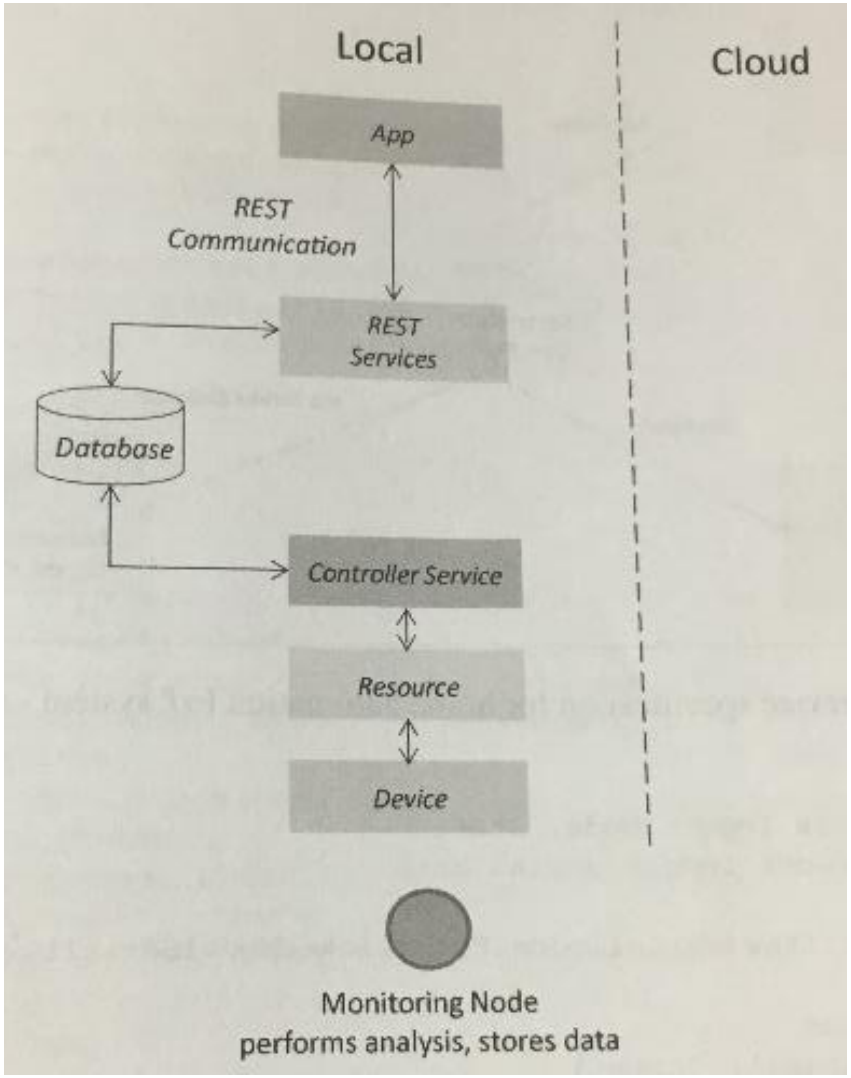
Smart Lighting

A design of a smart home automation system:

- **Control** the **lights** in a typical home remotely using a web application.
- The system include **auto** and **manual** modes.

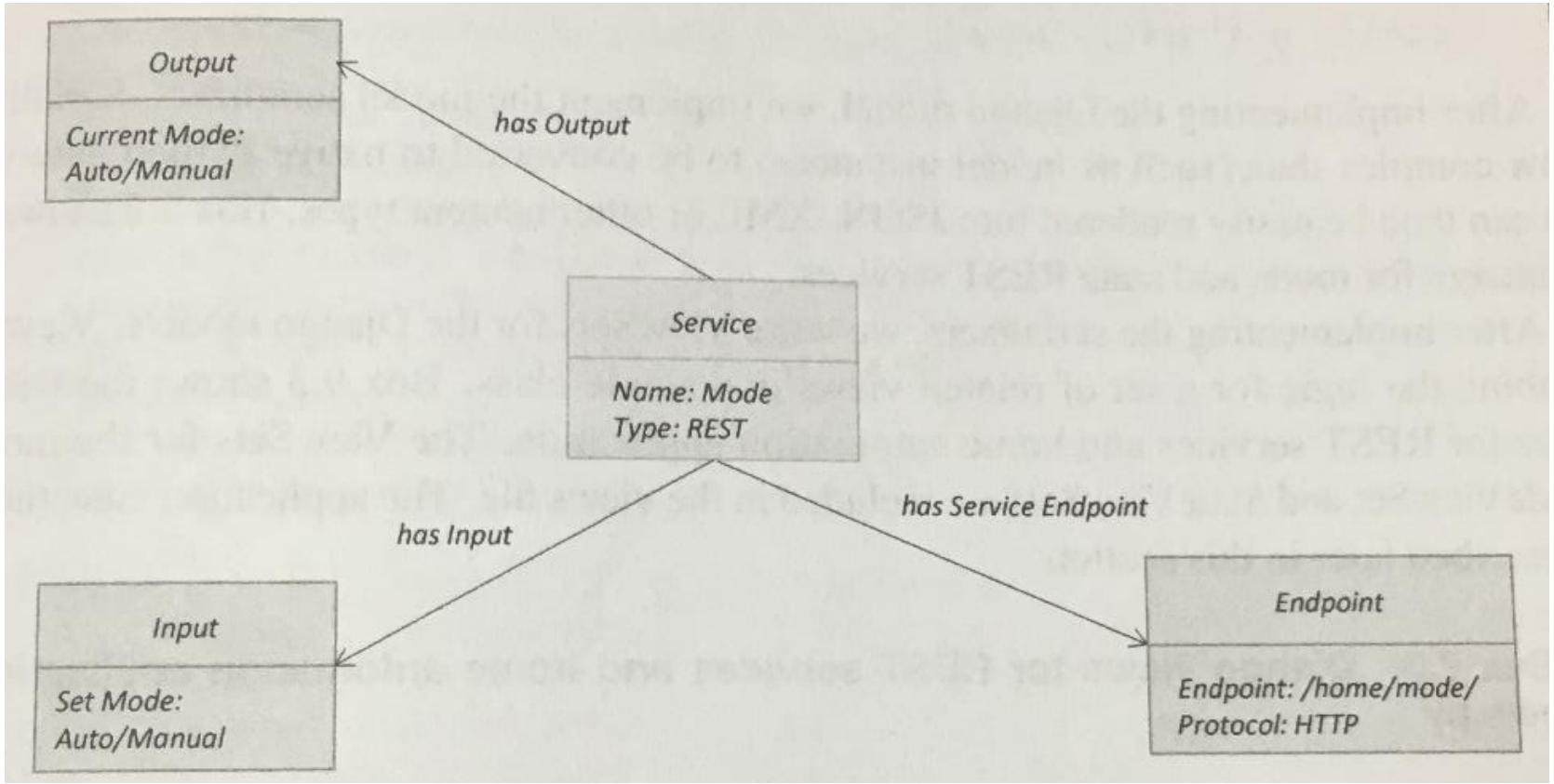
Smart Lighting

- Deployment design



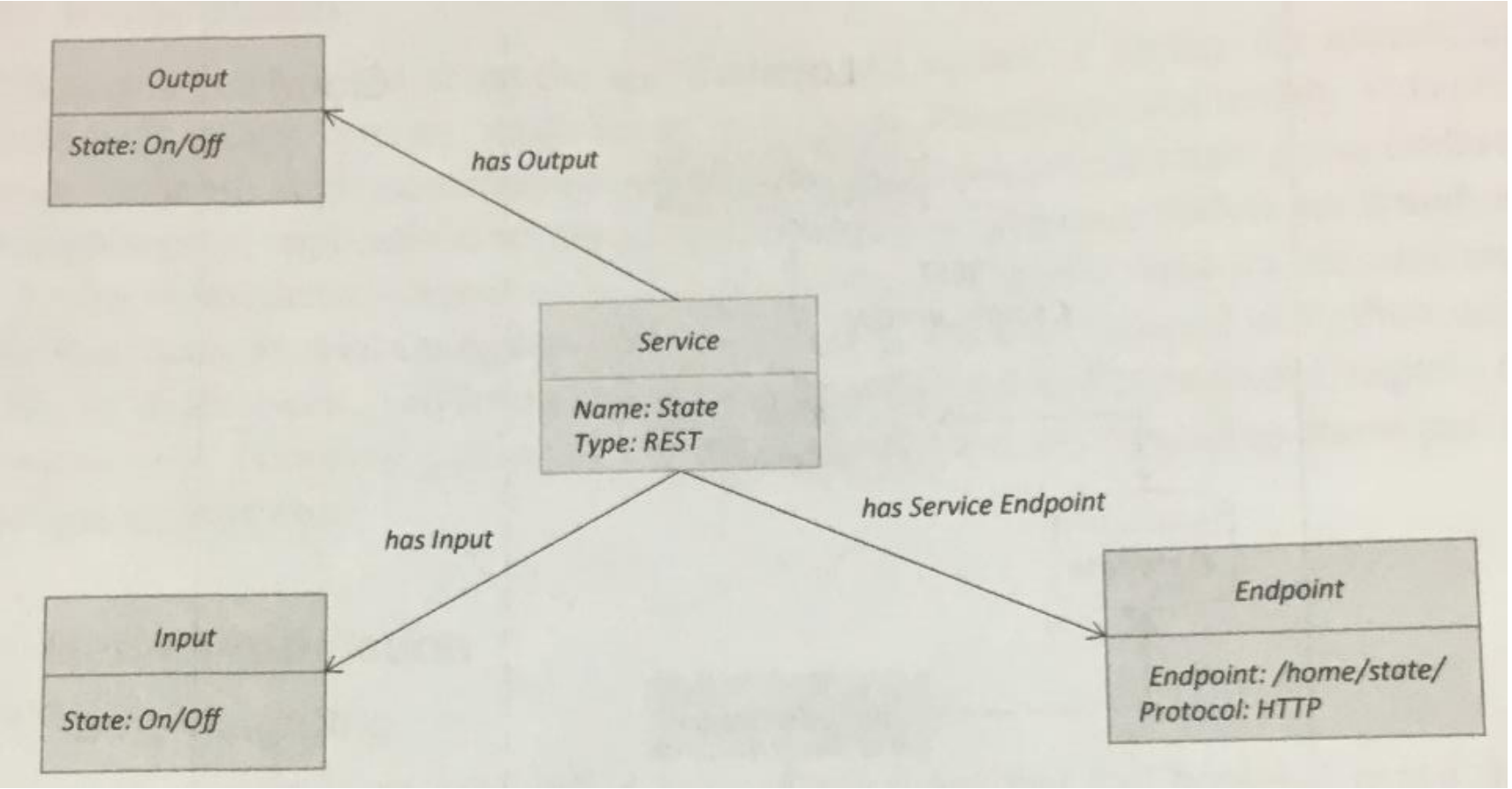
Smart Lighting

- Mode service



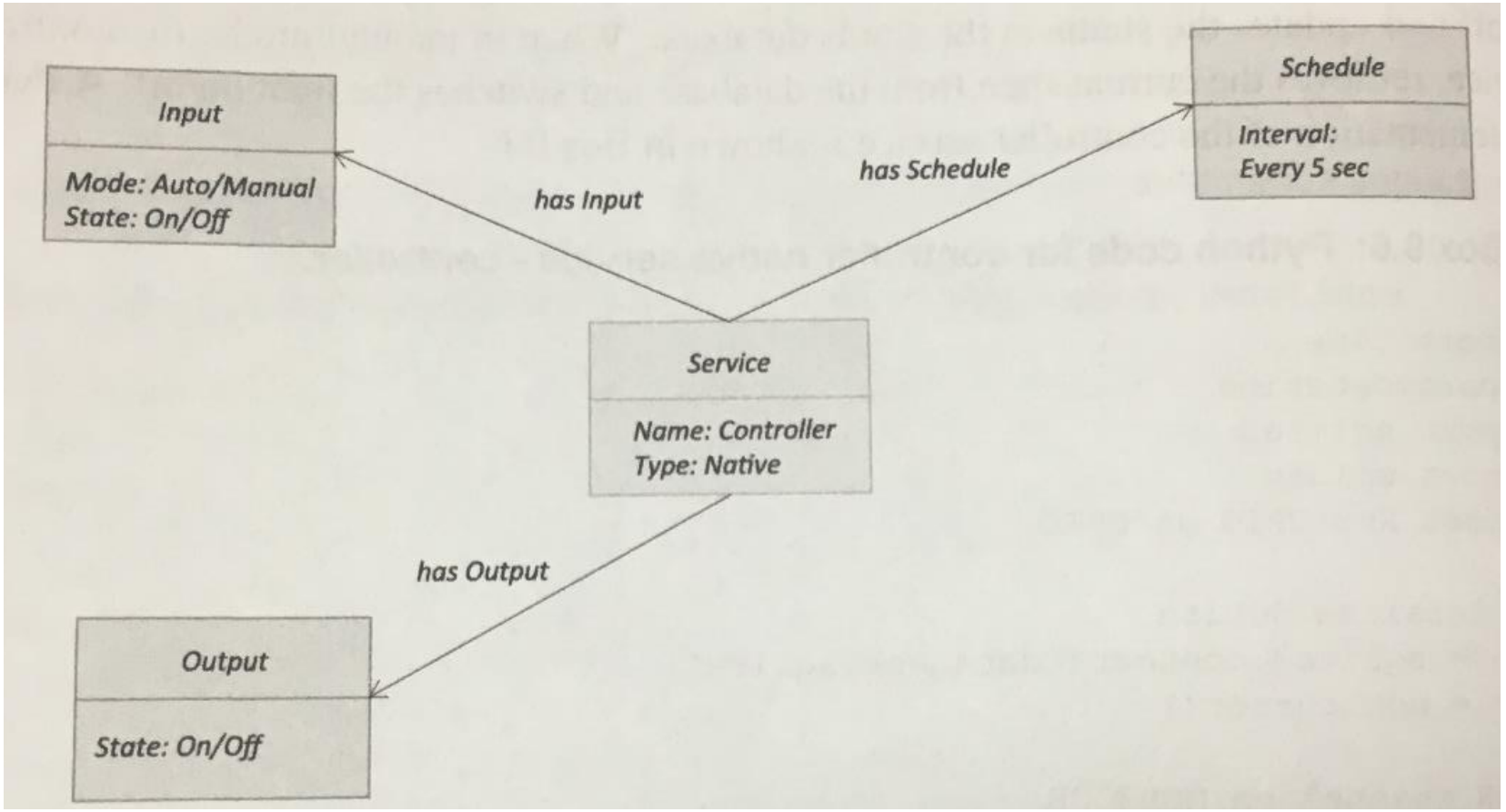
Smart Lighting

- State service



Smart Lighting

- Controller service



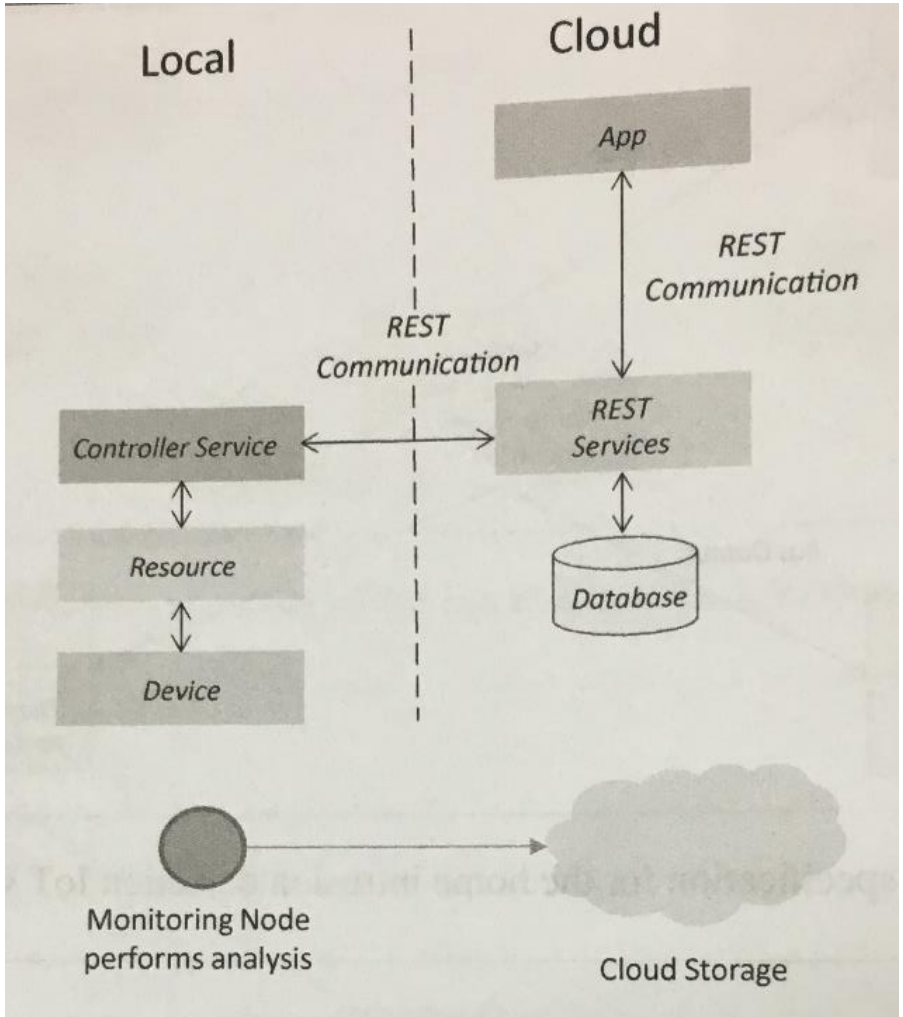
Home Intrusion Detection

A design of home intrusion detection systems:

- **Detect intrusions** using sensors and **raise alerts**, if necessary.
- Each **door** has a door sensor to **detect opening of door**.
- Each **room** has a PIR motion sensor to **detect motion**.

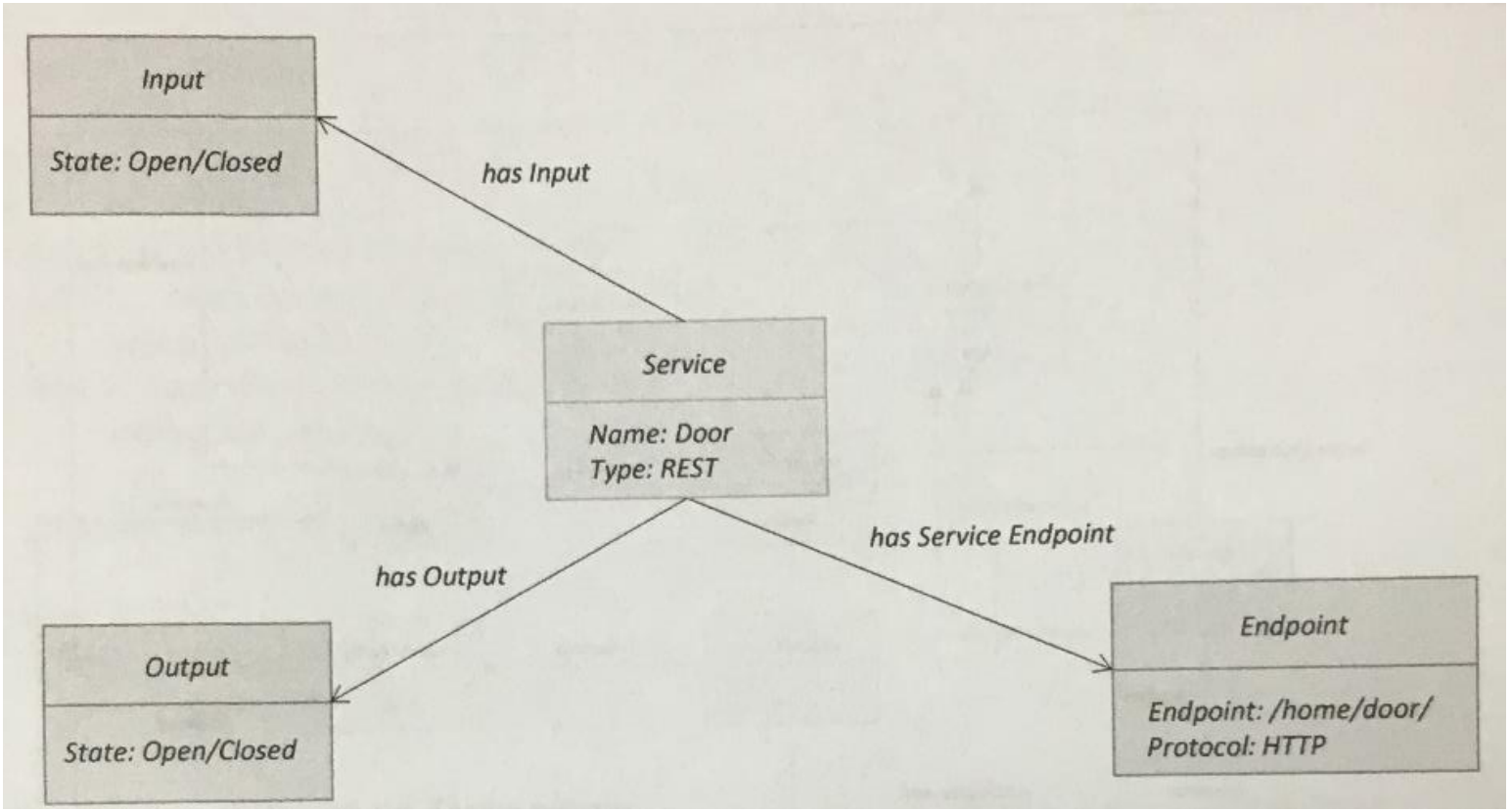
Home Intrusion Detection

- Deployment design



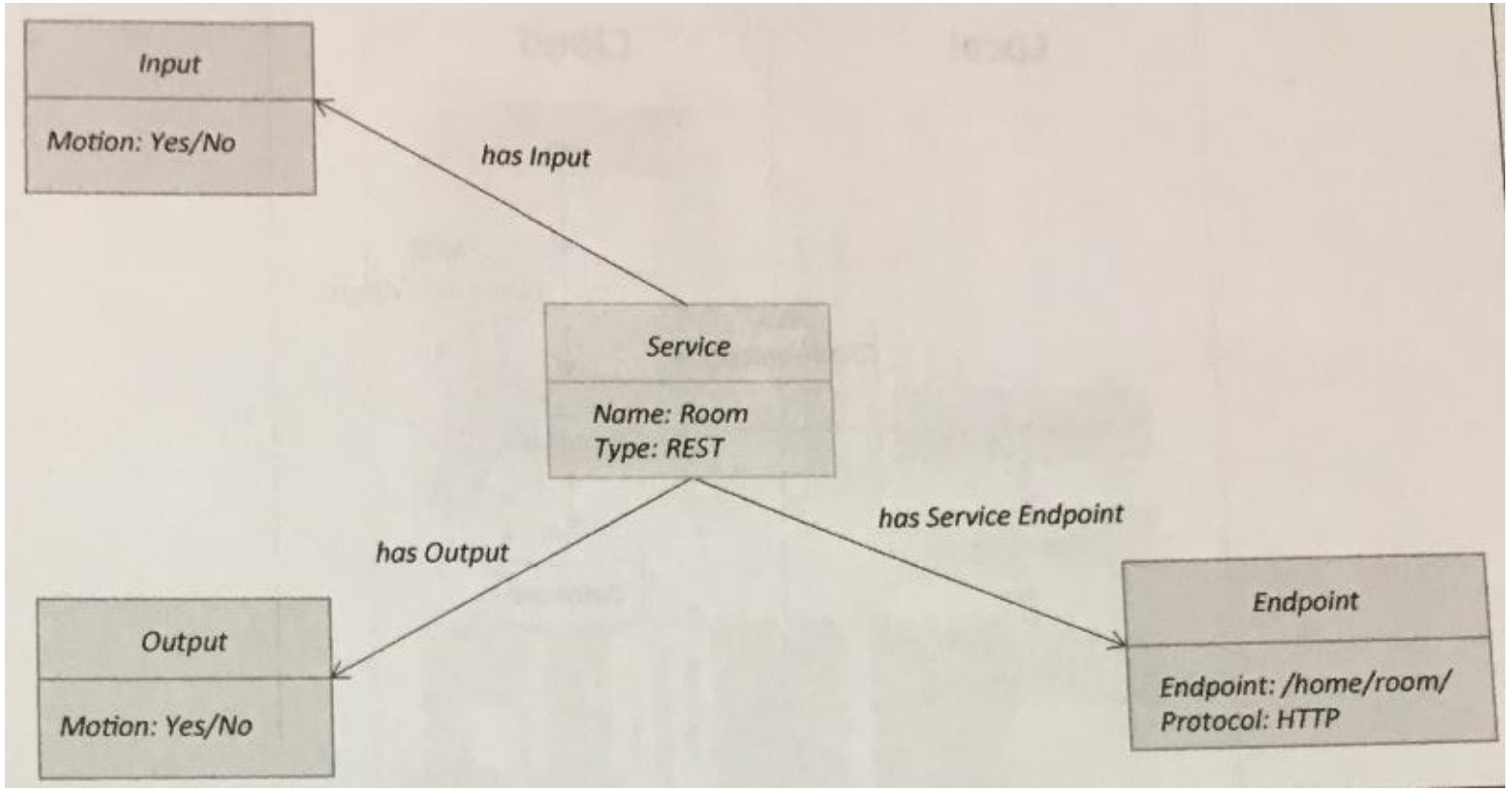
Home Intrusion Detection

- Door service



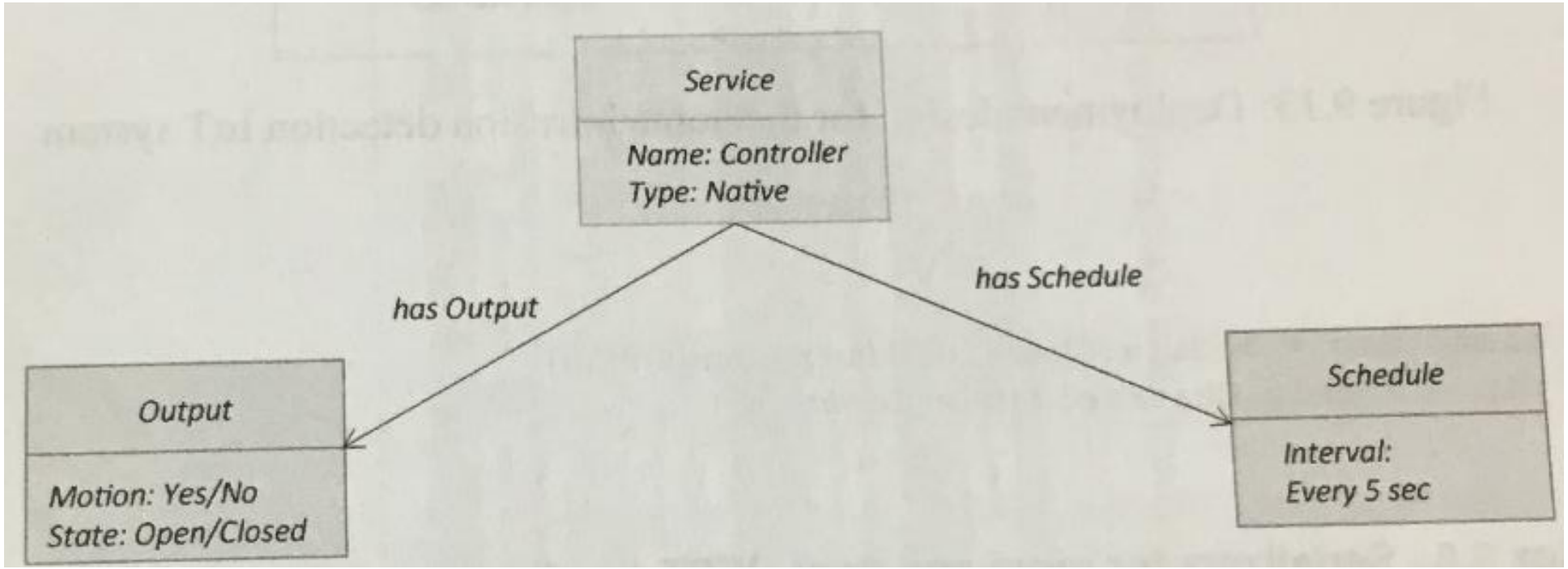
Home Intrusion Detection

- Room service



Home Intrusion Detection

- Controller service



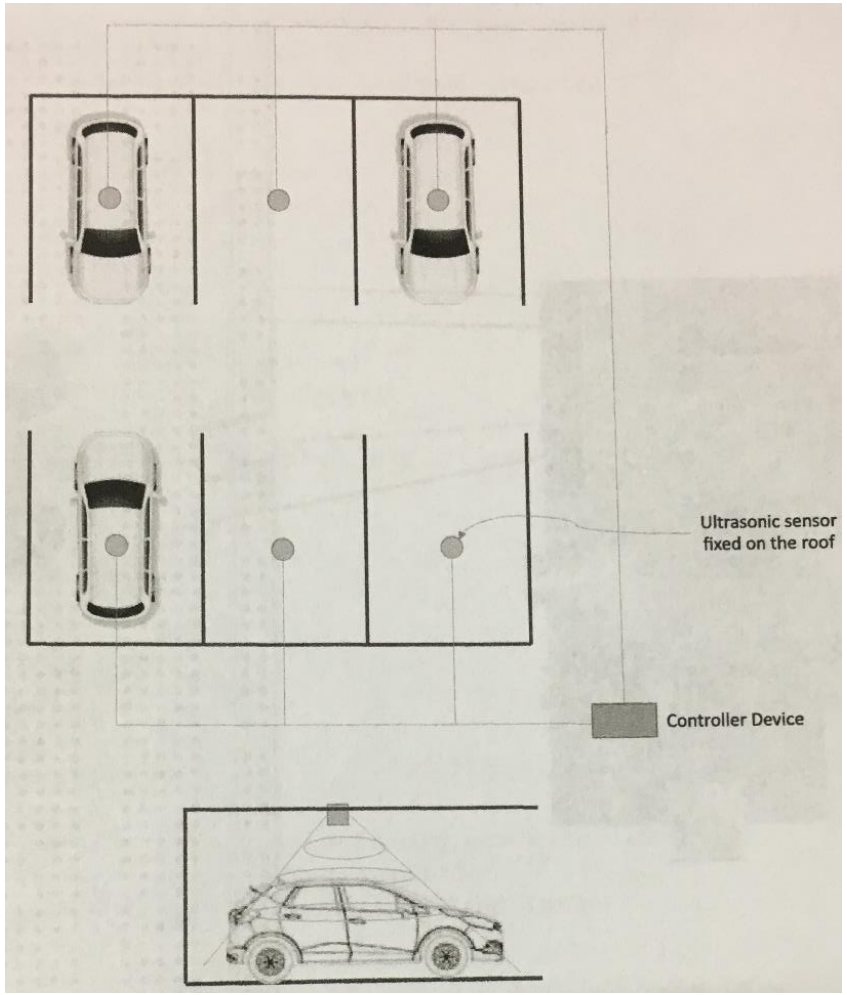
Smart Parking

A design of smart parking systems:

- Detect the number of empty parking slots to help drivers search parking space easily.
- Each parking slot have a sensor to detect whether the slot is empty or occupied.

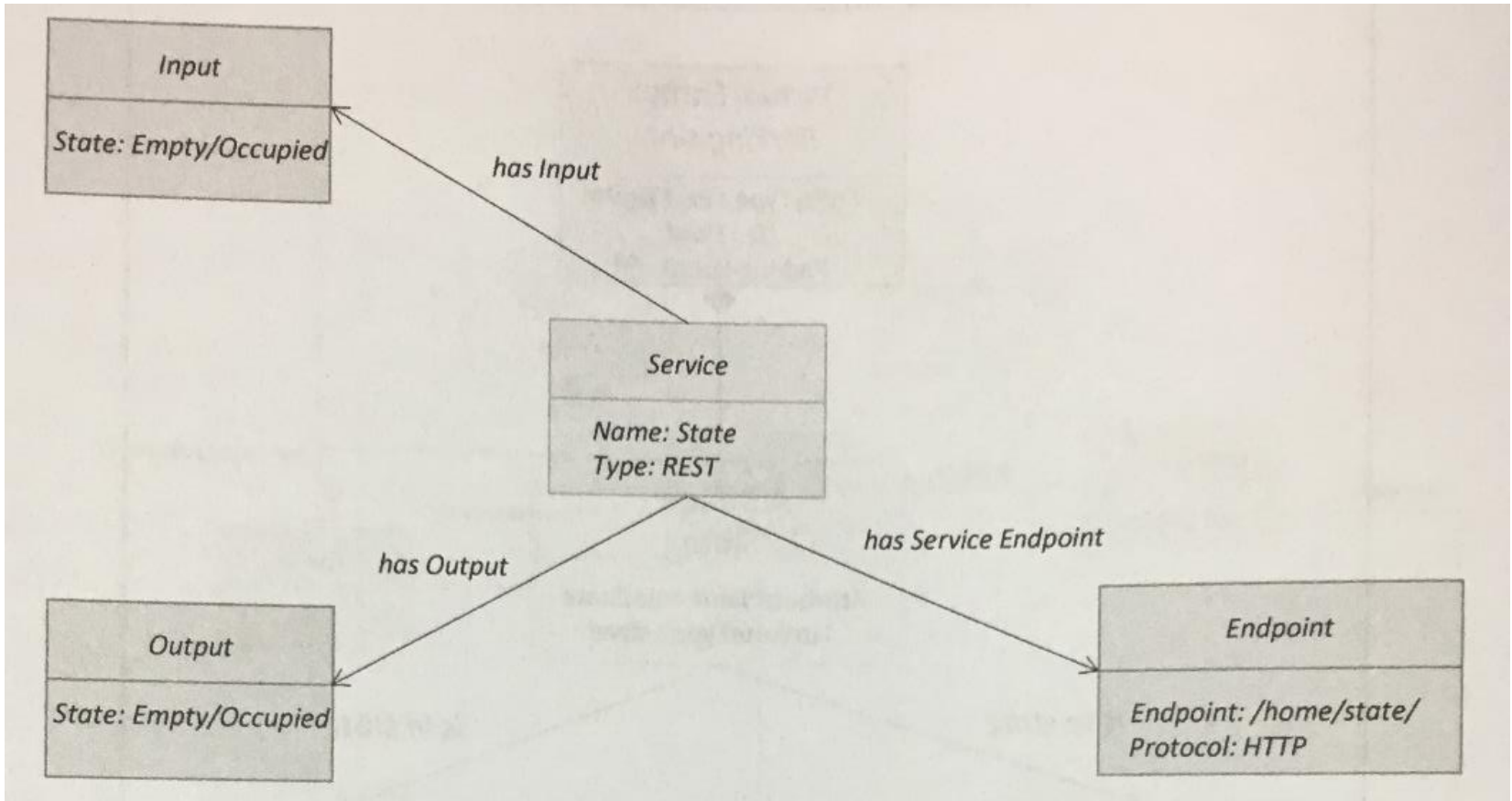
Smart Parking

- Deployment of sensors



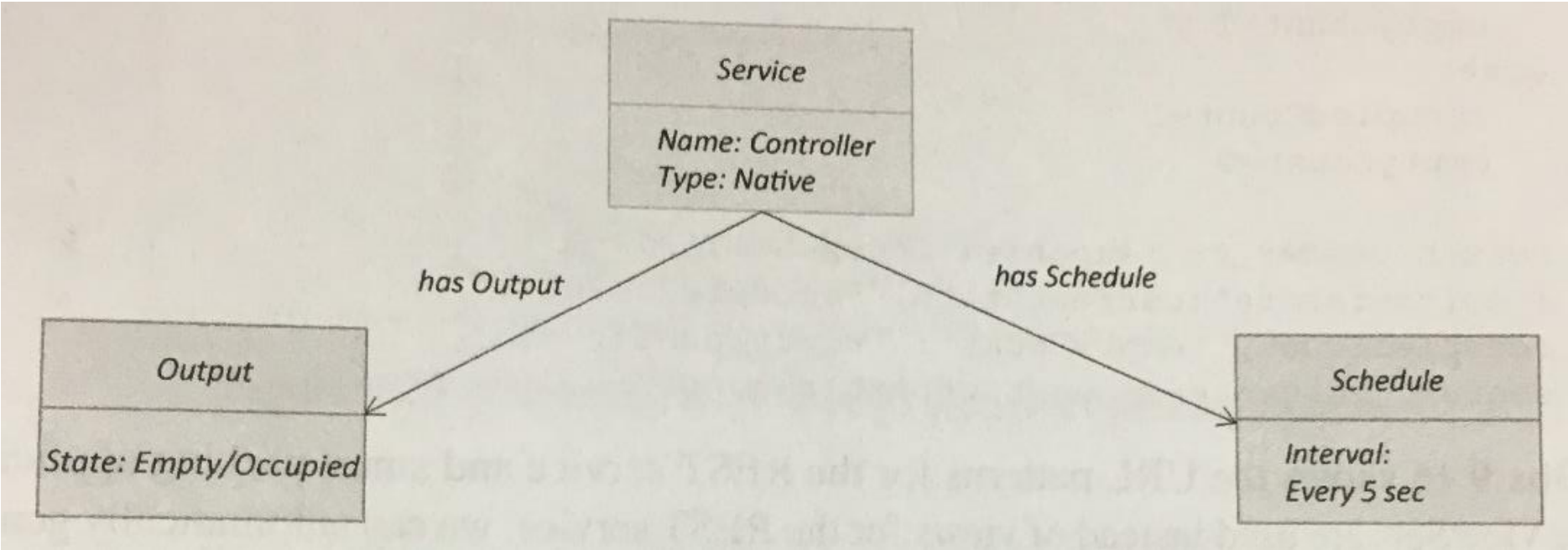
Smart Parking

- State service



Smart Parking

- Controller service



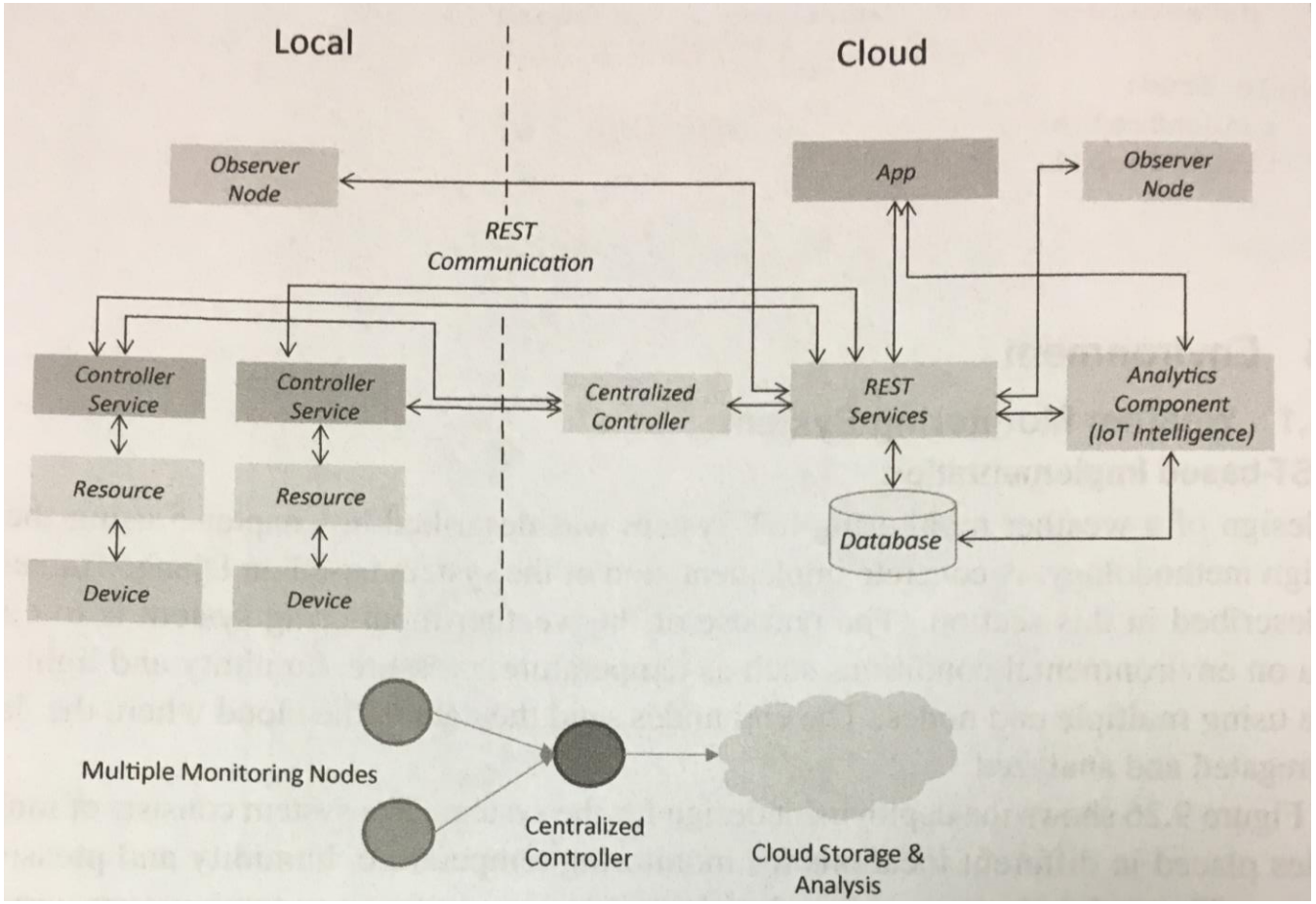
Weather Monitoring System

A design of a weather monitoring IoT system:

- Collect data on environmental conditions such as temperature, pressure, humidity and light in area using multiple end nodes.
- The end nodes send the data to the cloud where the data is aggregated and analyzed.
- The end nodes are equipped with various sensors (such as temperature, pressure, humidity and light).

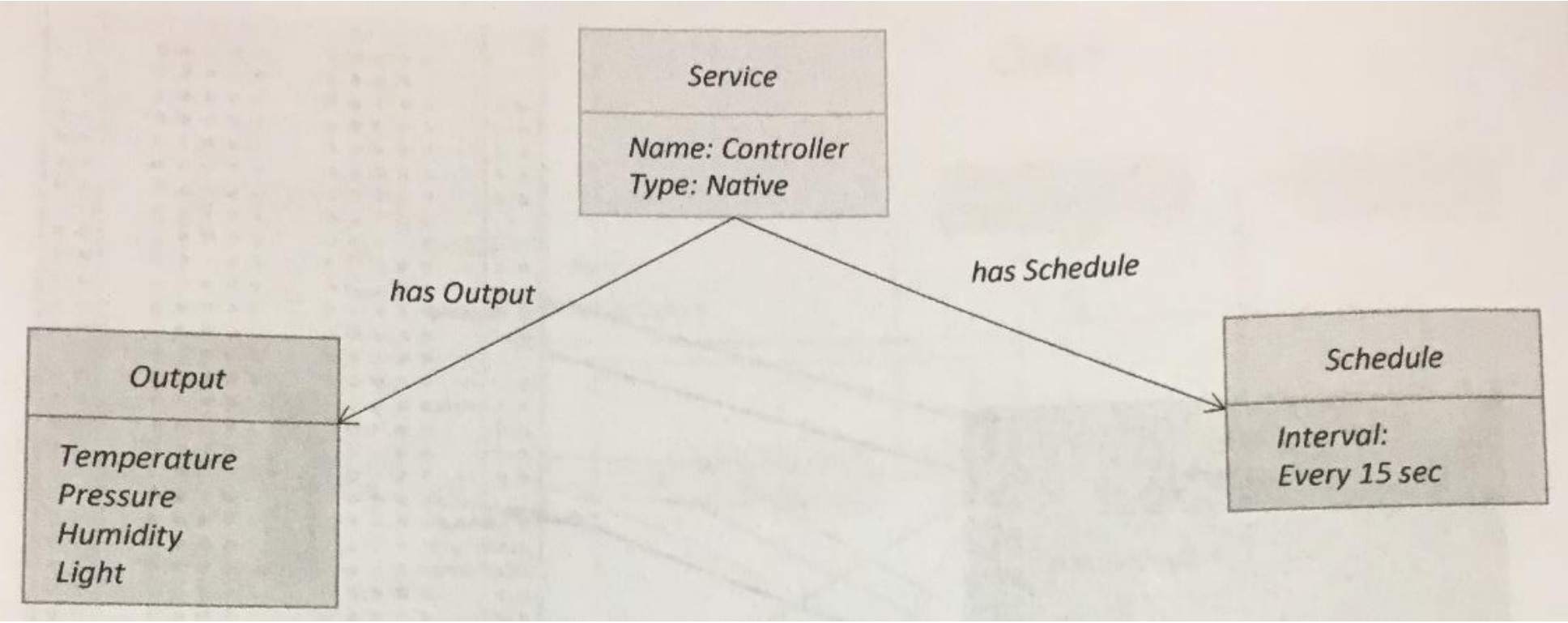
Weather Monitoring System

- Deployment design



Weather Monitoring System

- Controller service



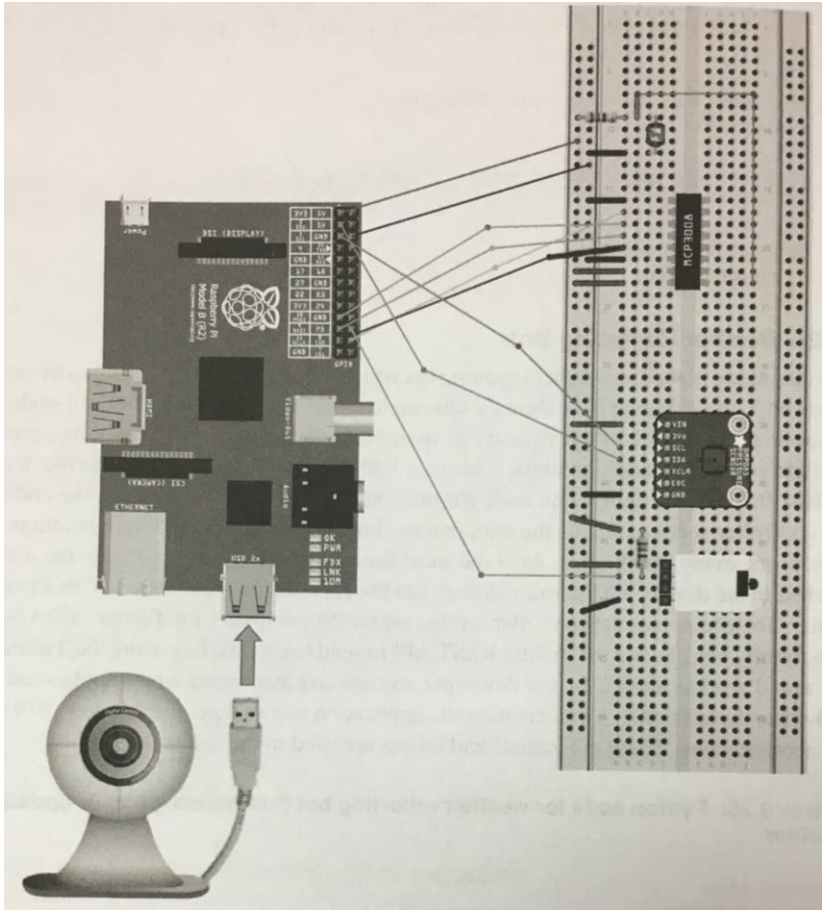
Weather Reporting Bot

A design of a weather reporting bot:

- Report weather information by sending tweets on Twitter.
- The end nodes are comprised of a Raspberry Pi mini-computer, temperature, pressure, humidity and light sensors. In addition to the sensors, a USB webcam is also attached to the device.
- To send tweets:
  - Using a Python library for Twitter called *tweepy*.
  - With tweepy we can use the Twitter REST API to send tweets.

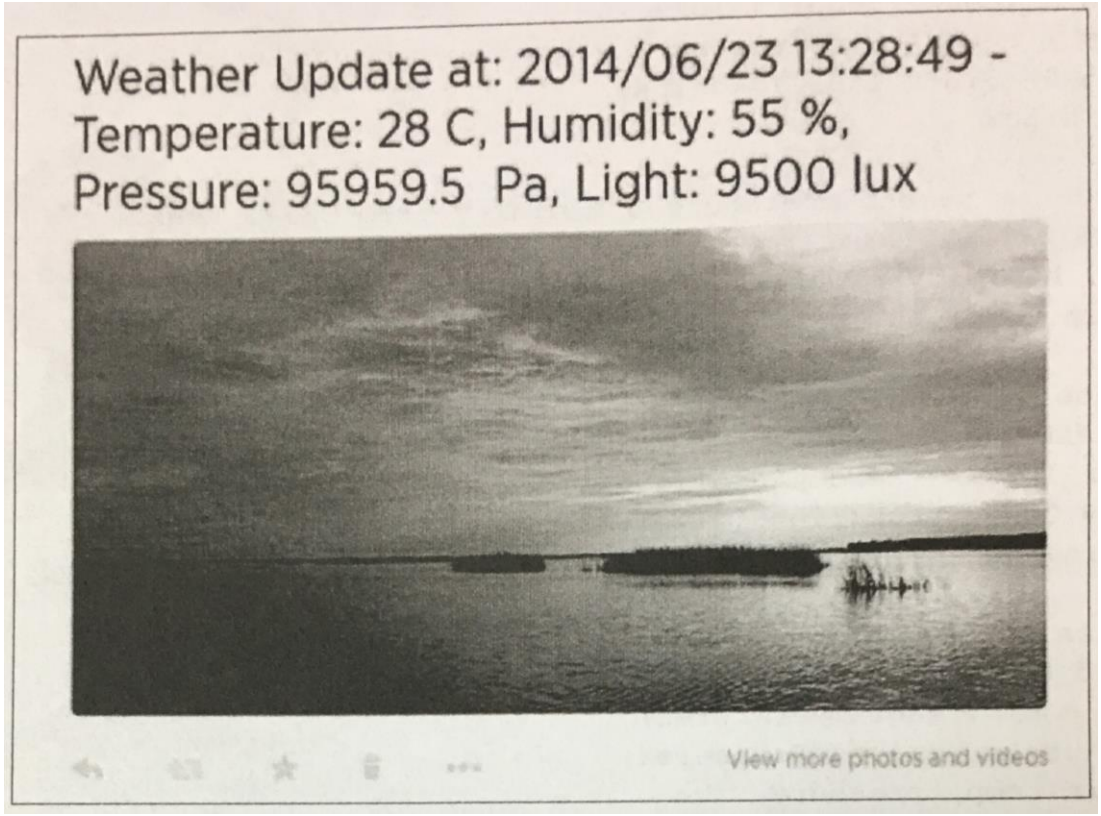
Weather Reporting Bot

- Schematic diagram – device and sensors.



Weather Reporting Bot

- Screenshot of a weather update tweeted.

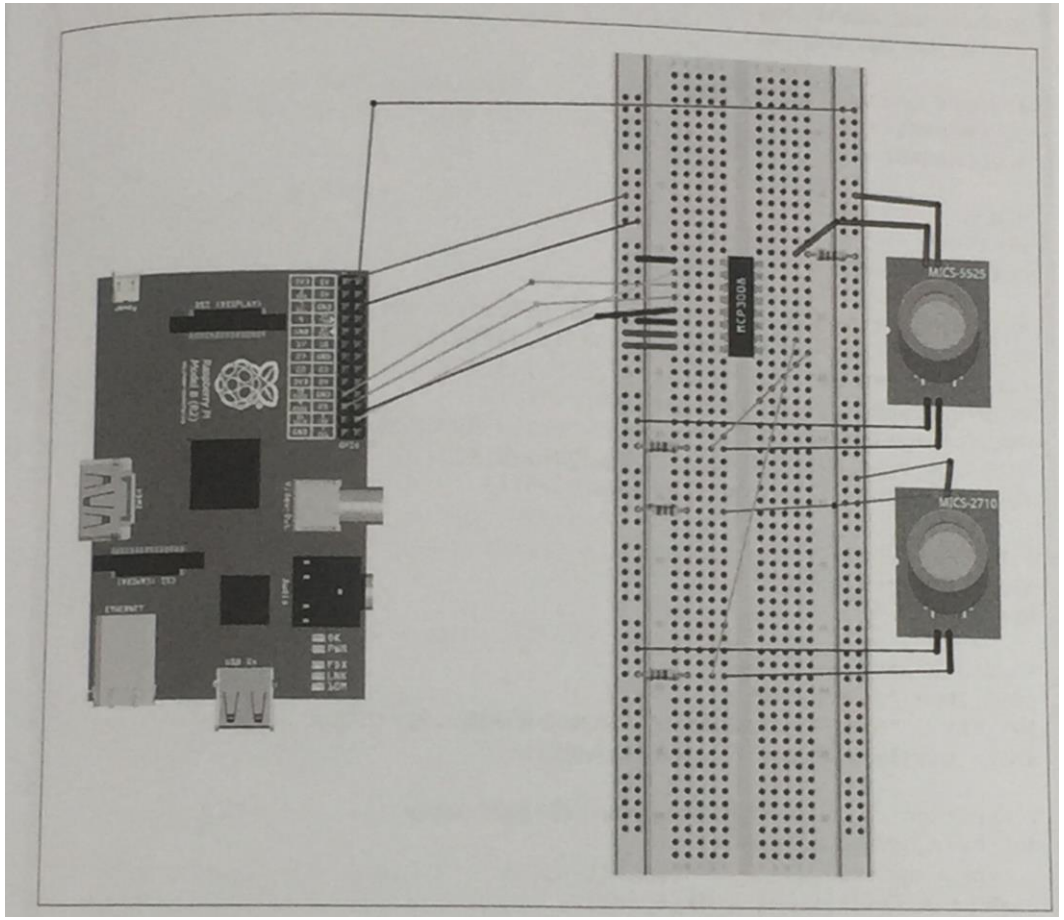


Air Pollution Monitoring

A design of an air pollution monitoring:

- Multiple nodes placed in different locations for monitoring air pollution in an area.
- End nodes: CO and NO_2 sensors
- Send data to the cloud database
- Visualizing the data with cloud-based application

Air Pollution Monitoring

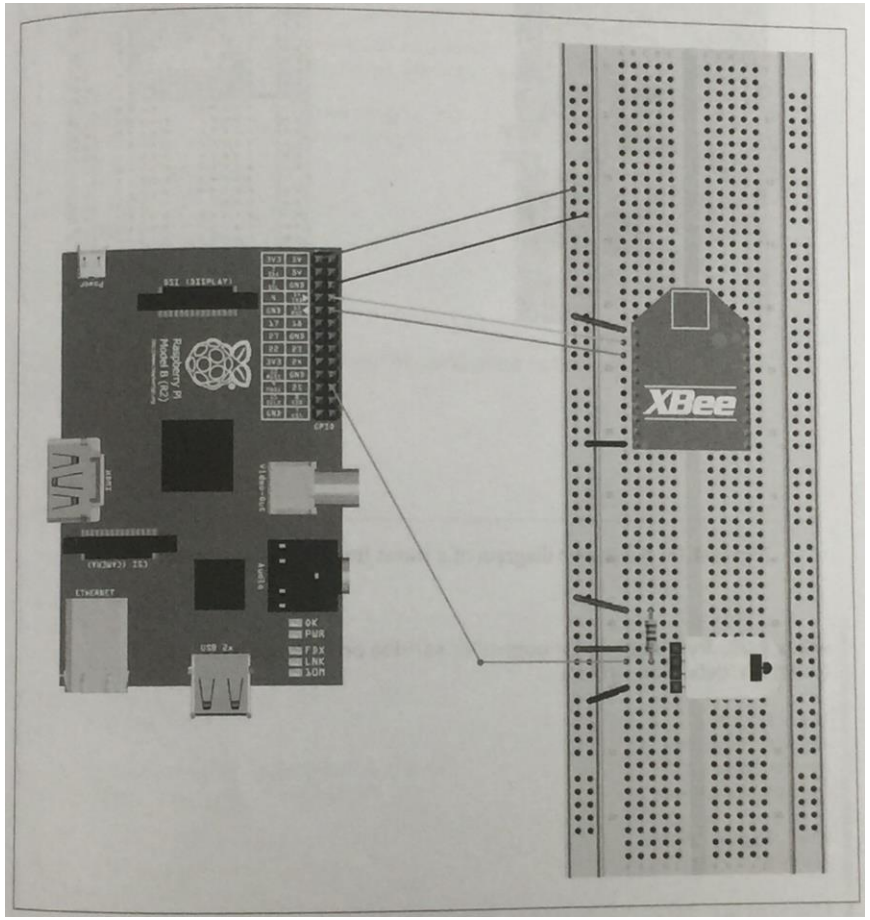


Forest Fire Detection

A design of a forest fire detection:

- A number of monitoring nodes (end nodes) deployed at different locations in a forest.
- End nodes collect measurements (like temperature and humidity) to predict whether a fire has broken out.
- Use one coordinator node to collect all data from end nodes through XBee module.
- Coordinator service calls rest api to send data to cloud.

Forest Fire Detection

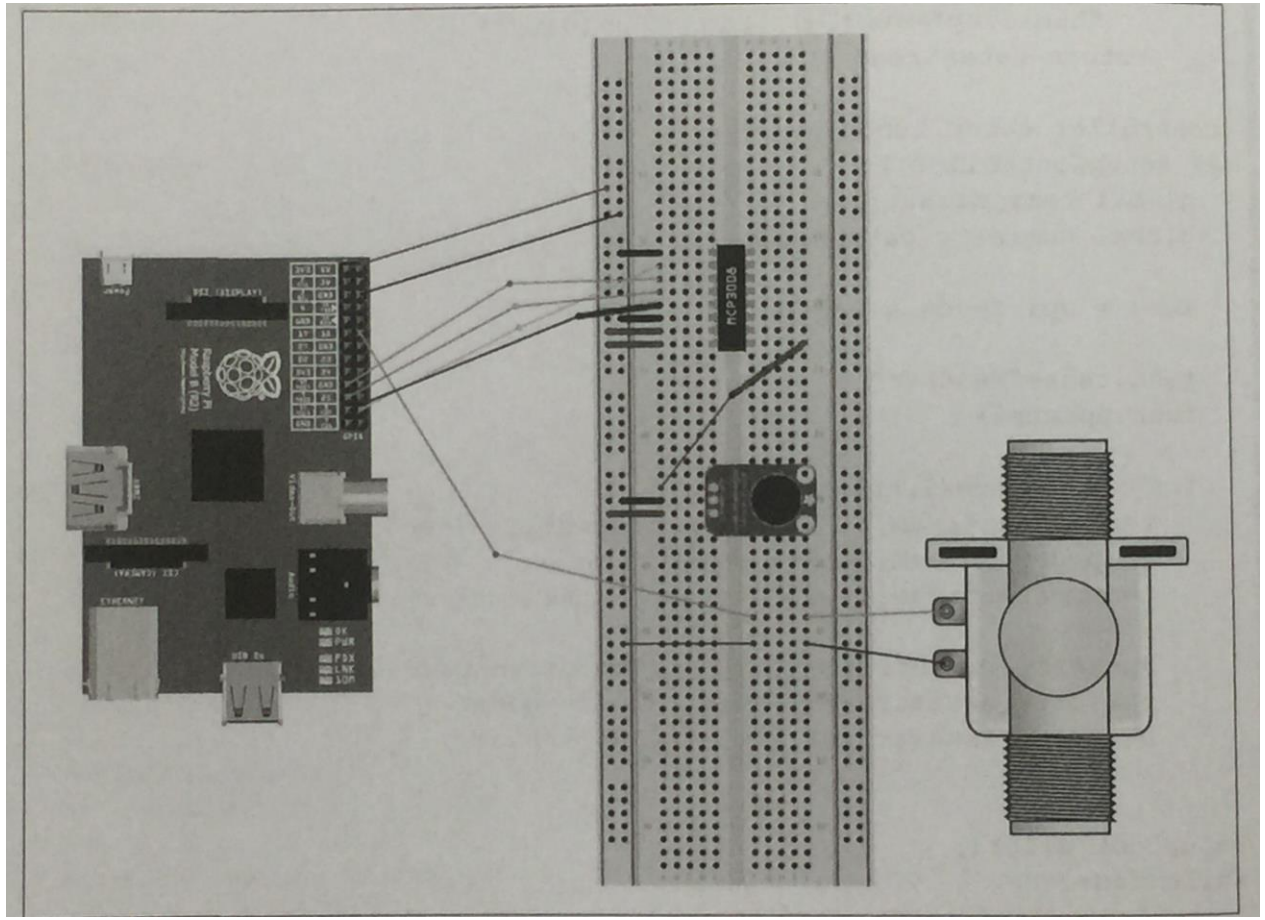


Smart Irrigation

A design of a smart irrigation:

- Multiple monitoring nodes (end nodes) placed in different locations for monitoring soil moisture.
- End nodes send data to cloud through Raspberry Pi.
- Cloud-based application visualize the data.
- A solenoid valve is used to control the flow of water, which connects to Raspberry Pi.

Smart Irrigation



IoT Printer

A design of an IoT printer:

- Fetch daily briefing information (today's weather prediction, …) on the Internet.
- Login to the google calendar to fetch your schedule.
- Write to a file and then print every morning.

IoT Printer