INTERNET OF THINGS (IOT)

Asst. Prof. DR. MUHANED TH. M. AL-HASHIMI

Tikrit University

Collage Of Computer And Mathematical Science

2024 - 2025

CONCEPTS OF IOT NETWORKING

LECTURE (4)

2204 - 2025

4 Of March

Lecture outline

Concepts of IoT Networking

1. IoT Networking
2. IoT Networking Components
3. Types of Networks
4. Devices
5. Sensors
6. Sensors Classify
7. Actuators and Controllers
8. Gateways

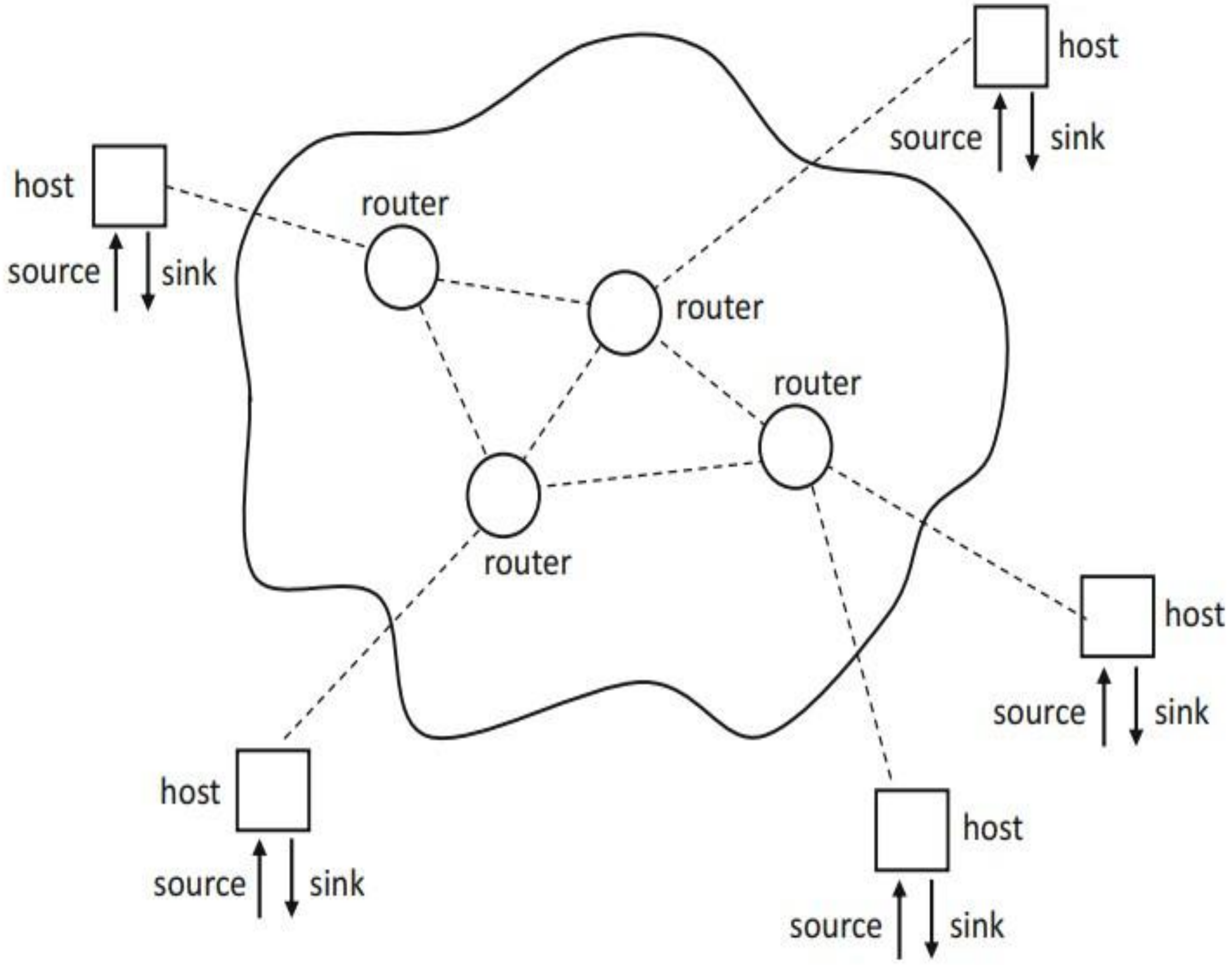
IoT Networking

- From a **functional** perspective, an IoT network, like most packet-switched networks, is **made of two types of devices**:

1. **endpoints** that are known as **hosts** and are the **source** or **destination** of messages.
2. **routers** that assist in the propagation of messages throughout the network.

- Both, **hosts** and **routers**, **form** communication systems with transmitters and receivers connected to channels by means of **links**.

- Each **router** supports **multiple hosts** that, in turn, are connected to **sources** and **sinks**



IoT Networking

- **In the context of IoT**, **hosts** are typically sensors, actuators, controllers, and devices in general as well as applications like those performing complex decision-making.
- Routers, on the other hand, can be **dedicated equipment** or **other devices**.
- By giving **plain devices**, like sensors and actuators, routing capabilities, it is possible to **lower** deployment times and costs by **maximizing** hardware reutilization.

IoT Networking

- **Links**, depending on the **nature of the channel**, can be wireless associated with free propagation, or wireline associated with guided propagation.
- **In the context of IoT**, the **decision** between relying on wireless and relying on a wireline solution is related to device deployment **costs** and **times**.
- in order to support a **massive number of devices**, wireline solutions usually require huge infrastructure changes that are too expensive and take too long to implement.
- Wireless architectures with **battery-powered** devices are the most common type of IoT deployment.
- **Alternatively**, wireline scenarios that **take advantage** of preexistent power wiring for communications are also popular.

IoT Networking

- One **important consideration** is that a transmitted signal is affected by channel noise. By the time the signal arrives at the receiver, it has been attenuated and affected by channel noise leading to a specific signal-to-noise (SNR).

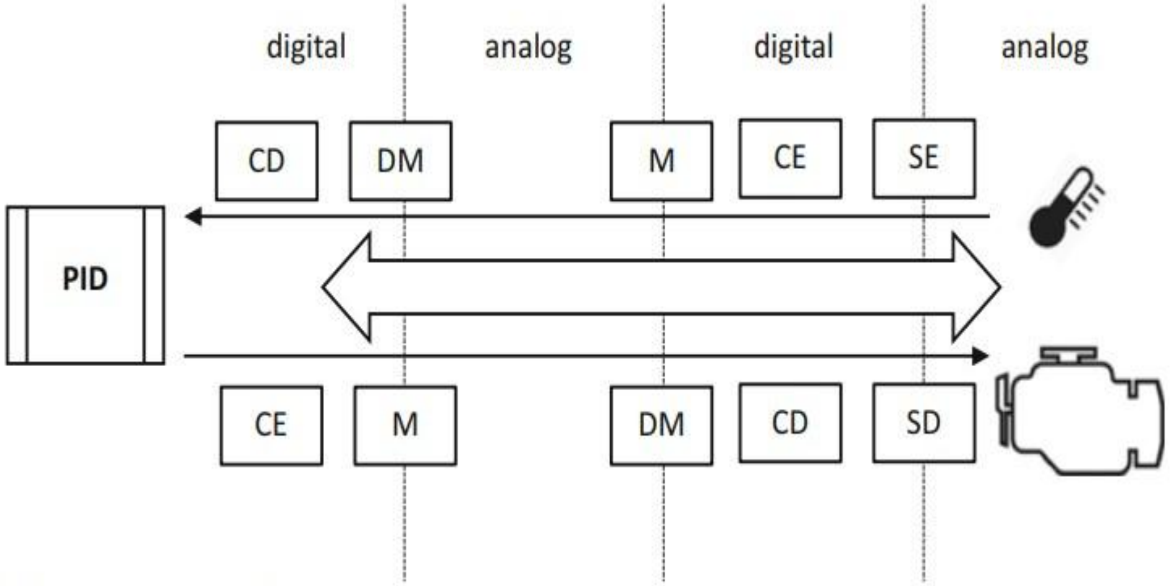
- Higher SNR typically means higher transmission Rates.

- **In IoT networks**, this can be **challenging** as preserving battery life usually implies low signal power and low SNR which translates into **low** transmission rates.

- cause **IoT devices**, like sensors, to interact with the physical environment, they monitor infinite precision analog assets like temperature, humidity, or light intensity that cannot be **packetized** and **transmitted** without certain transformations.

IoT Networking

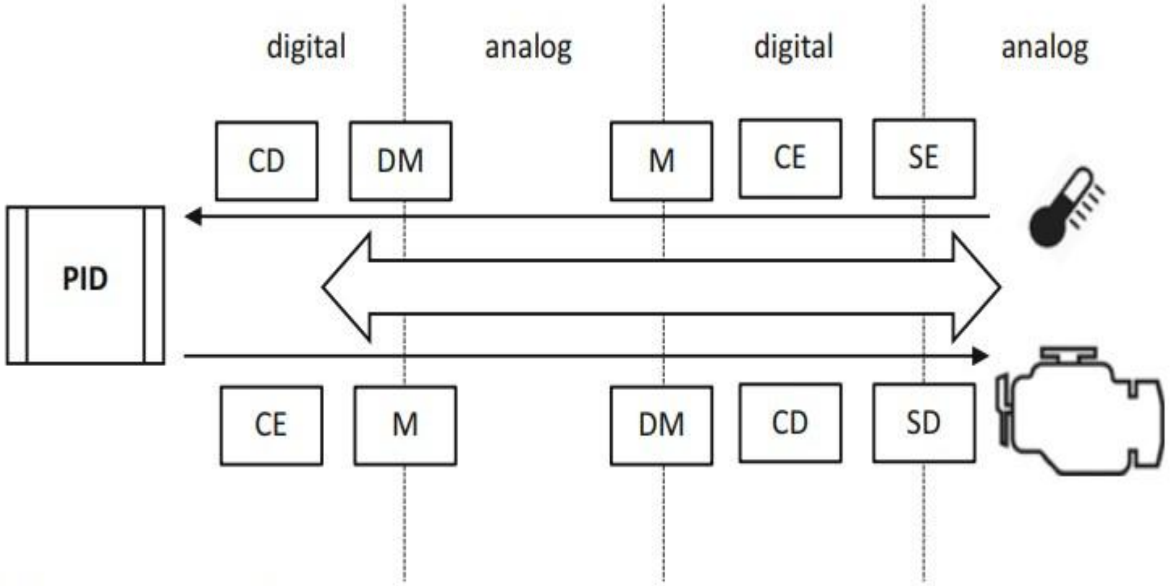
- in the context of a **layered architecture**, **first**, the analog variable is converted to a digital number represented by a sequence of bits generated by source encoding at **Analog to Digital Converter (ADC)**.
- **The converted digital value** representing the asset can then be prepared for transmission by **adding** reliability, addressing, and additional routing information as part of channel encoding.
- This is typically done by appending headers and other fields to **the converted digital value** in order to build a packet in a way that is consistent with transport, network, and link layers.
- The **resulting packet** can then be transmitted over the channel as a modulated wave. Note that modulation is performed by the physical layer.



PID	PID controller
CD	channel decoder
DM	demodulator
M	modulator
CE	channel encoder
SE	source encoder
SD	source decoder
CD	channel decoder

IoT Networking

- Since the **channel is analog** because it exists in the physical world, modulation performs one more conversion. Essentially, the **modulator converts** the packet into electrical signals that can be transmitted through **wires** or propagated through **antennas**.
- When the **signal arrives** at the **receiver**, the demodulator, at the **physical layer**, restores the digital packet by converting the signal into a stream of **bits**.
- Subsequently, the **channel decoder** removes any address fields and additional reliability information performed at link, network, and transport layers, and it forwards the payload to the **application layer**.
- Since the **application** is an algorithm that is run by a piece of software, there is no need to convert the information any further. At this point, the **application** uses the temperature readouts as **samples** that can be processed by a generic **Proportional Integral Derivative (PID)** controller **algorithm**.



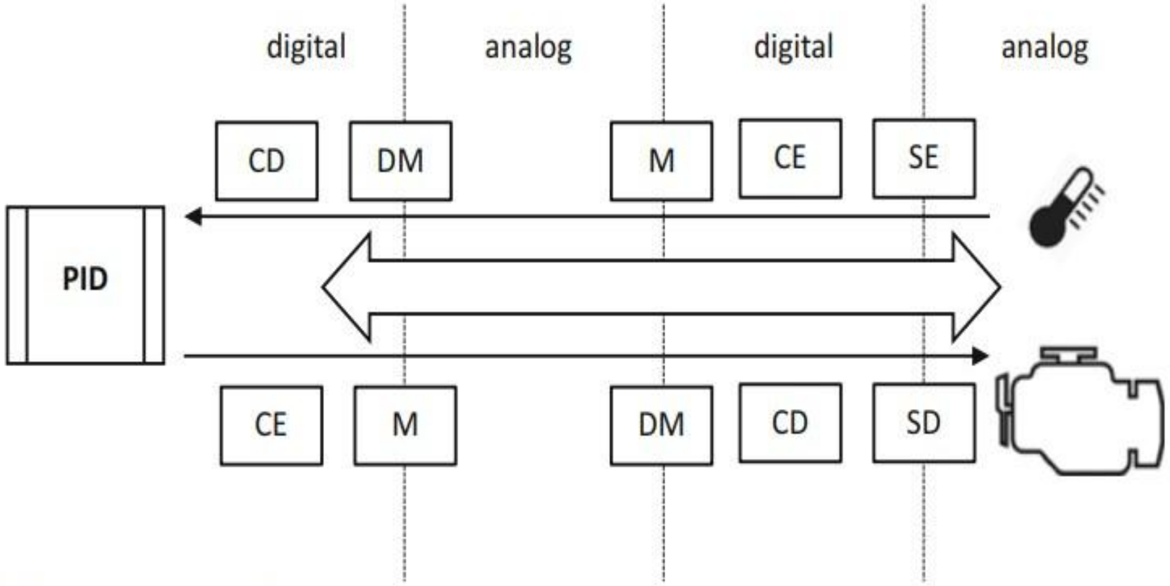
PID	PID controller
CD	channel decoder
DM	demodulator
M	modulator
CE	channel encoder
SE	source encoder
SD	source decoder
CD	channel decoder

IoT Networking

- **In sensing scenarios**, the consumer of the payload is an application that makes automated decisions.

- **In actuation scenarios**, however, digital data is generated by an application and transmitted through the channel to a device that performs actuation.

- In this case, since **the consumer** of the digital payload is **analog**, source decoding converts it into an analog signal by means of a Digital to Analog Converter (**DAC**).



PID	PID controller
CD	channel decoder
DM	demodulator
M	modulator
CE	channel encoder
SE	source encoder
SD	source decoder
CD	channel decoder

IoT Networking Components

- An **IoT implementation** is composed of several components, which **may vary with their application domains**.
- Various established works such as that by Savolainen et al. generally outline five broad categories of IoT networking components.
- However, we outline the broad **components** that come into play during the establishment of any IoT network, into **six** types:
  1) IoT **node**.
  2) IoT **router**.
  3) IoT **LAN**.
  4) IoT **WAN**.
  5) IoT **gateway**.
  6) IoT **proxy**.

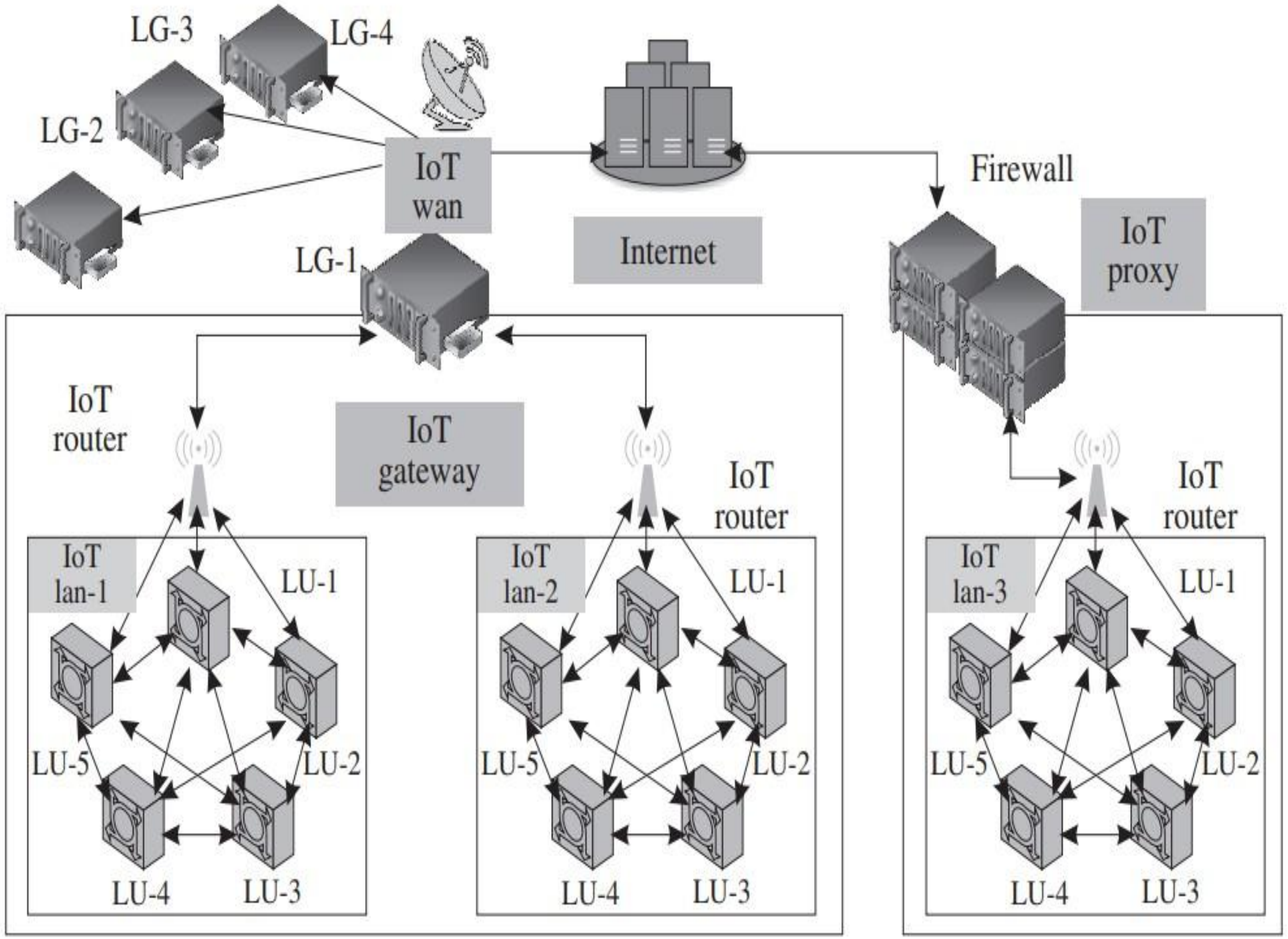


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

1) IoT **node**.
2) IoT **router**.
3) IoT **LAN**.
4) IoT **WAN**.
5) IoT **gateway**.
6) IoT **proxy**.

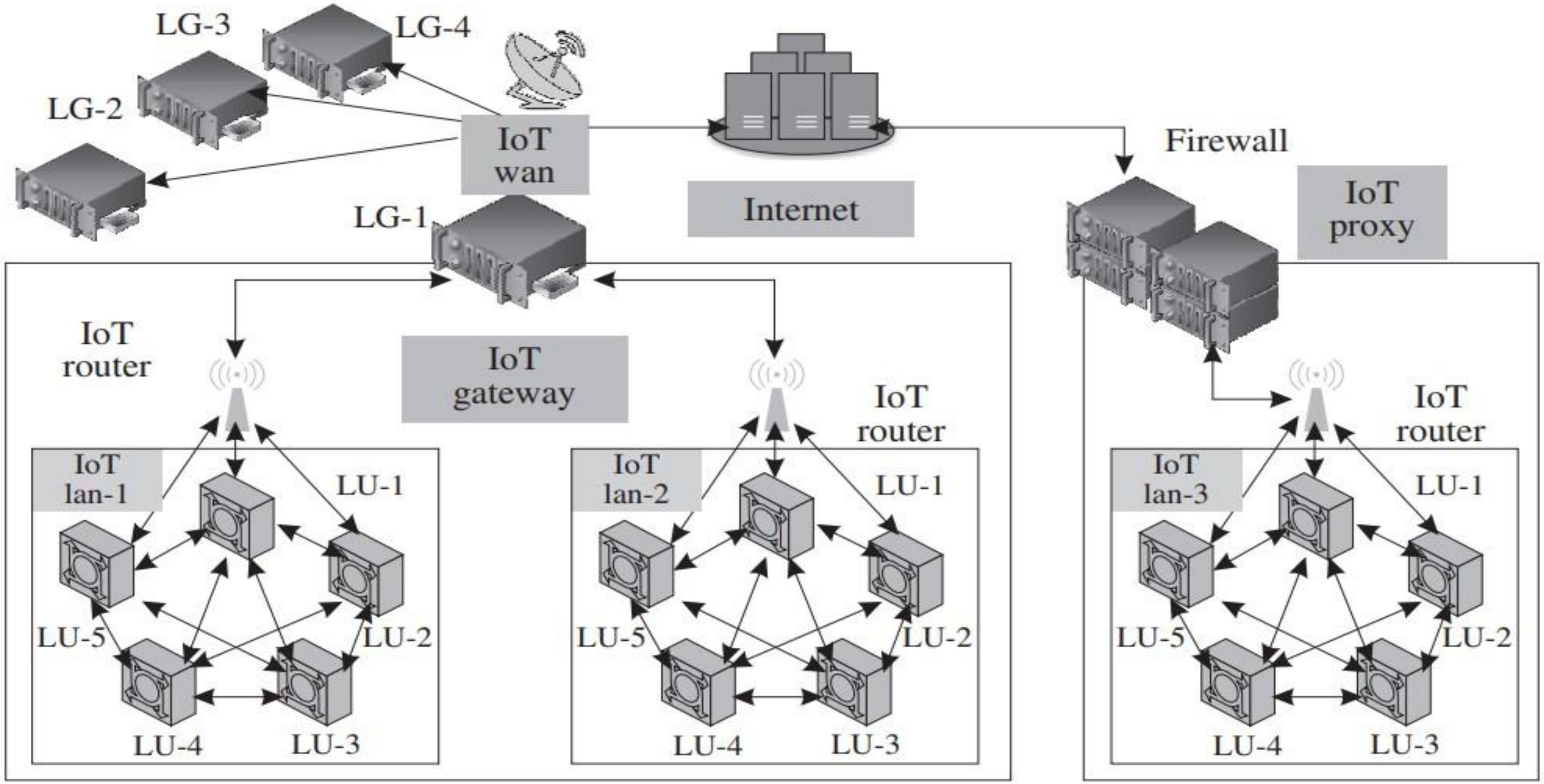


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

1) IoT node:

- ✓ These are the **networking devices** within an IoT LAN.
- ✓ Each of these devices is typically **made up** of a sensor, a processor, and a radio, which communicates with the **network infrastructure** (either within the LAN or outside it).
- ✓ The nodes may be connected to other nodes **inside a LAN** directly or by means of a common gateway for that LAN.
- ✓ Connections **outside** the LAN are through gateways and proxies.

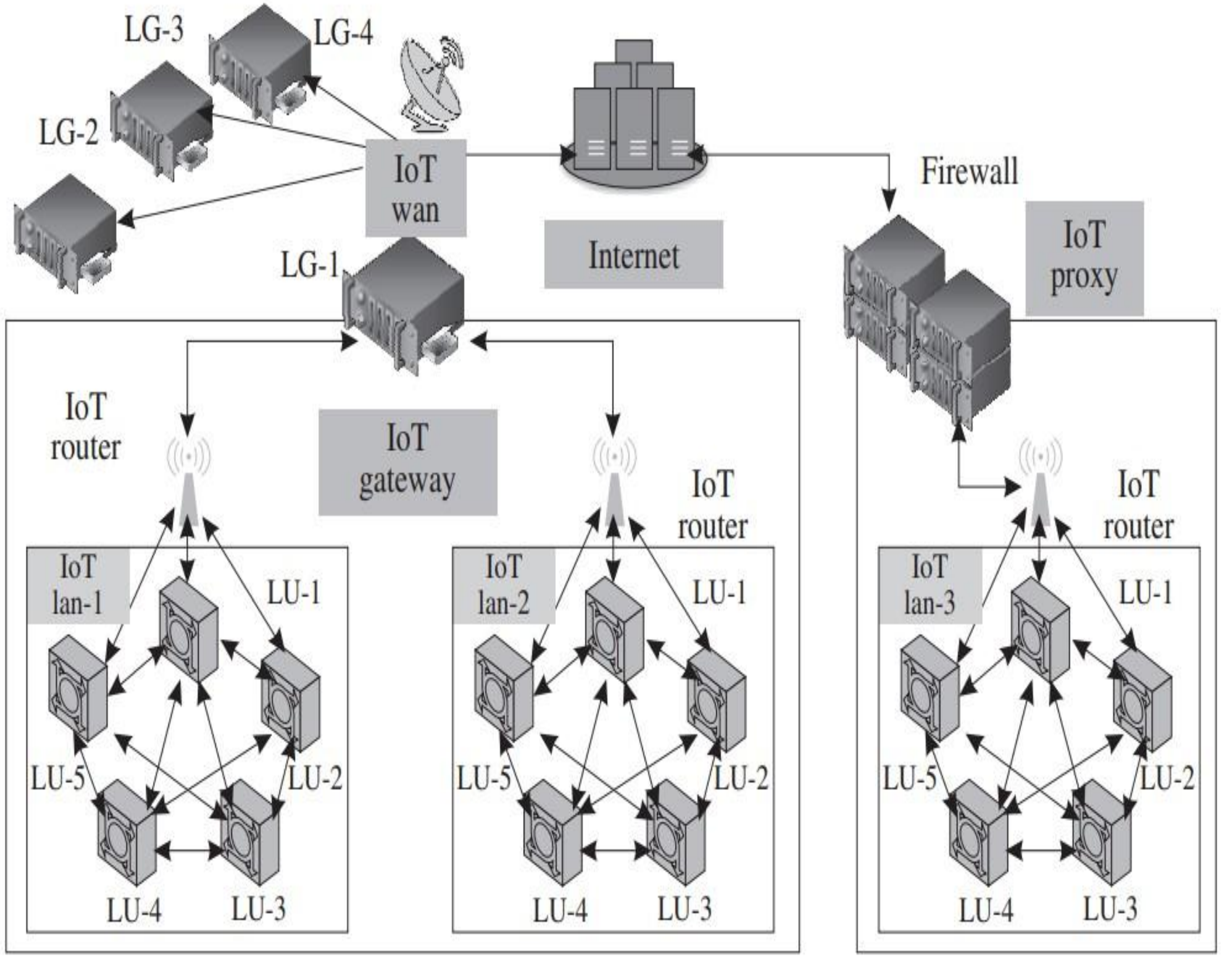


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

2) IoT router:

- ✓ An **IoT router** is a piece of networking equipment that is primarily tasked with the routing of packets between various entities in the IoT network; it keeps the traffic flowing correctly within the network.
- ✓ A **router can** be repurposed as a gateway by enhancing its functionalities.

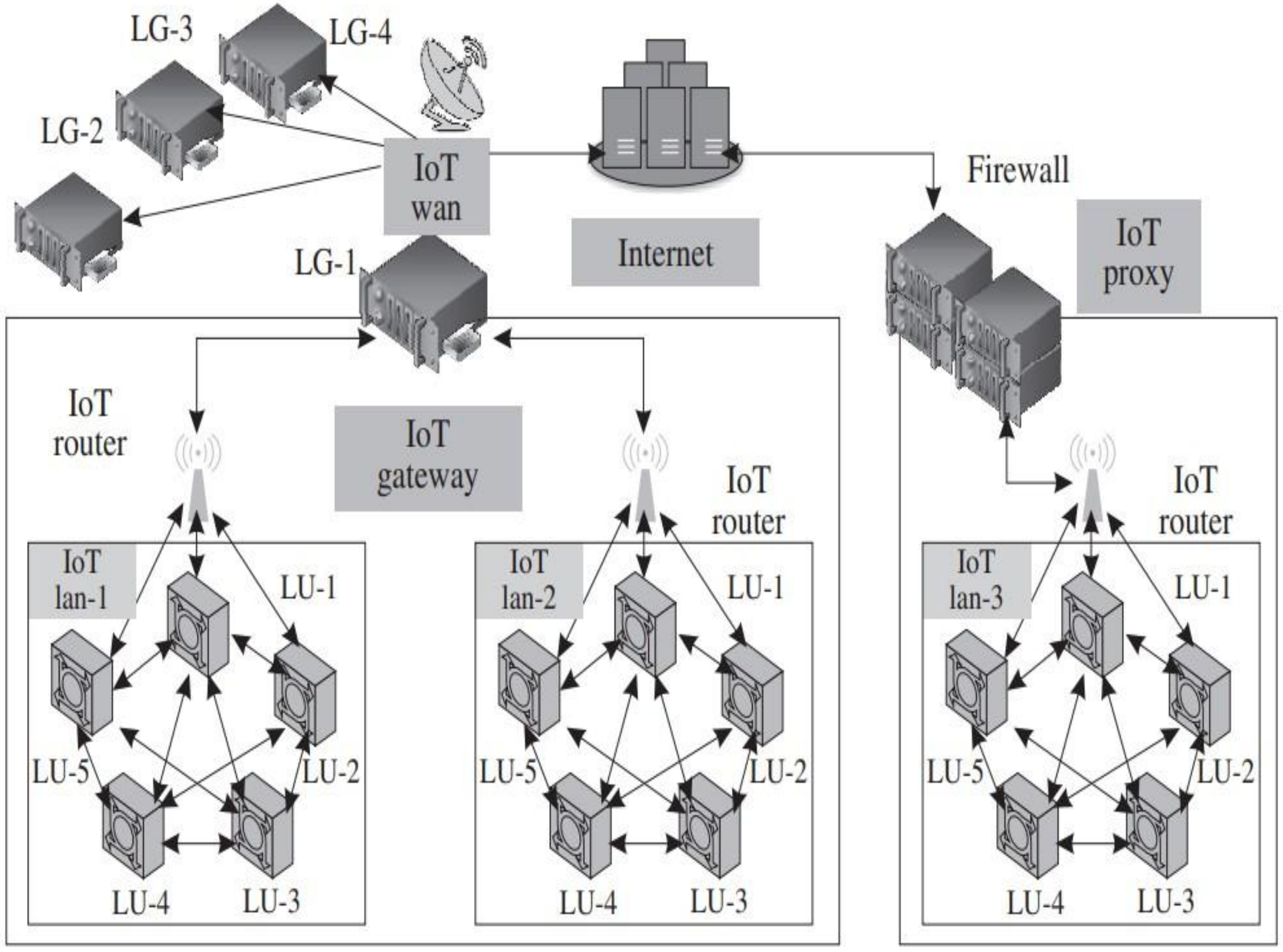


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

3) IoT LAN:

- ✓ The local area network (LAN) enables local connectivity within the purview of a single gateway.
- ✓ Typically, they consist of short-range connectivity technologies.
- ✓ IoT LANs may or may not be connected to the Internet.
- ✓ Generally, they are **localized** within a building or an organization.

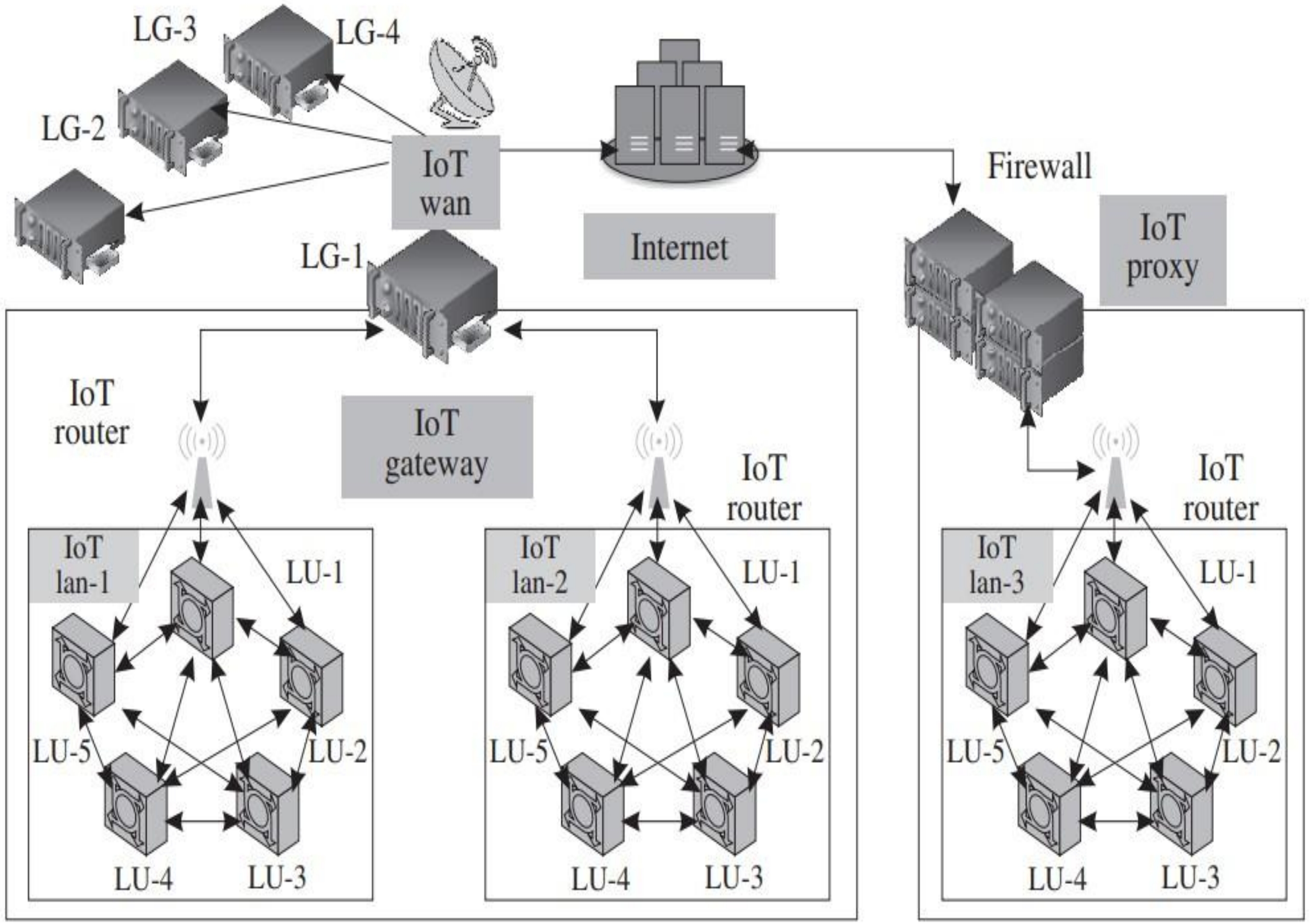


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

4) IoT WAN:

- ✓ The wide area network (WAN) connects various network segments such as LANs.
- ✓ They are typically organizationally and geographically wide, with their operational range lying between a few kilometers to hundreds of kilometers.
- ✓ IoT WANs connect to the Internet and enable Internet access to the segments they are connecting.

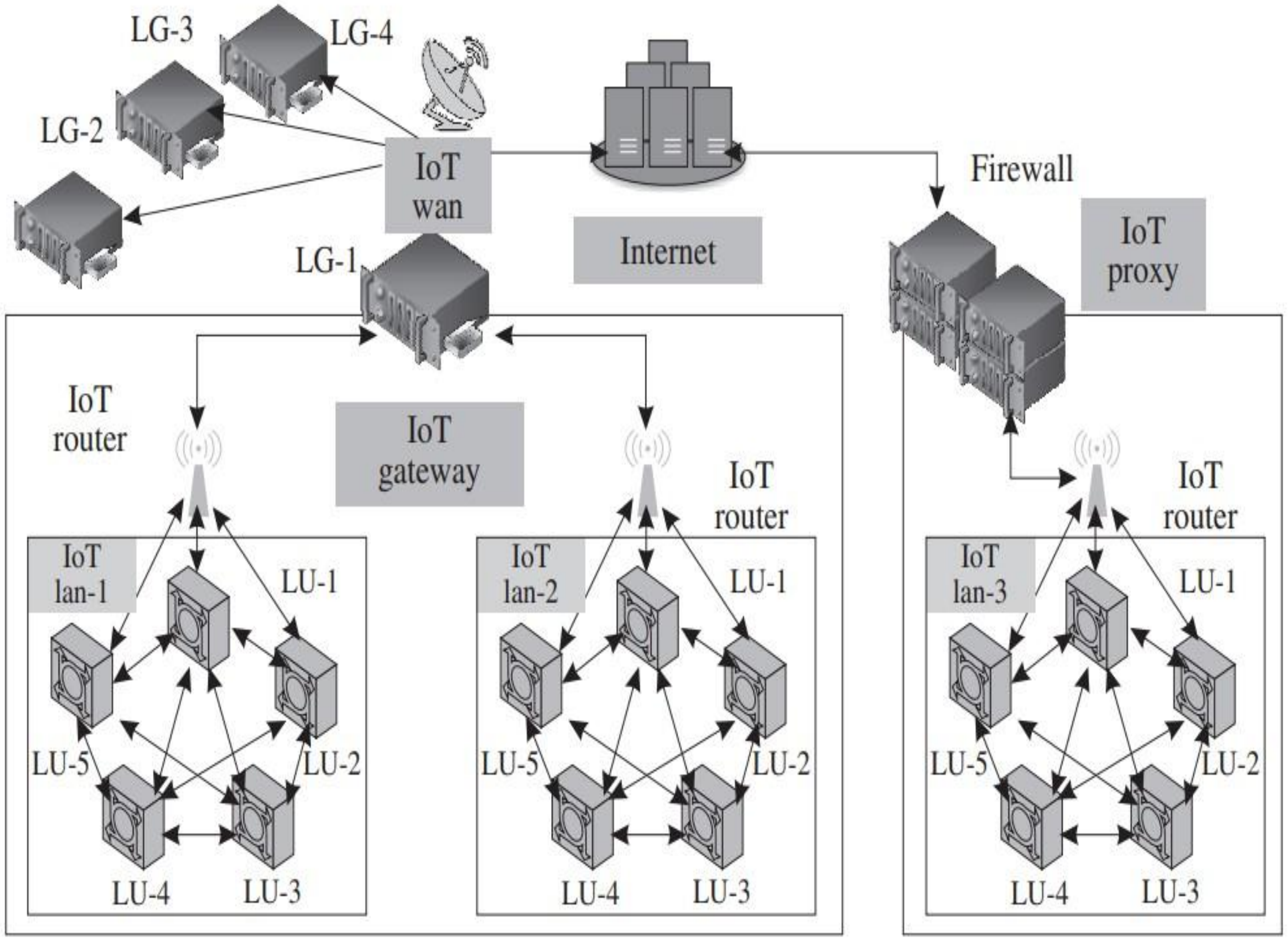


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

5) IoT gateway:

- ✓ An IoT gateway is simply a router connecting the IoT LAN to a WAN or the Internet.
- ✓ **Gateways** can implement several LANs and WANs.
- ✓ Their **primary task** is to forward packets between LANs and WANs, and the IP layer using only layer 3.

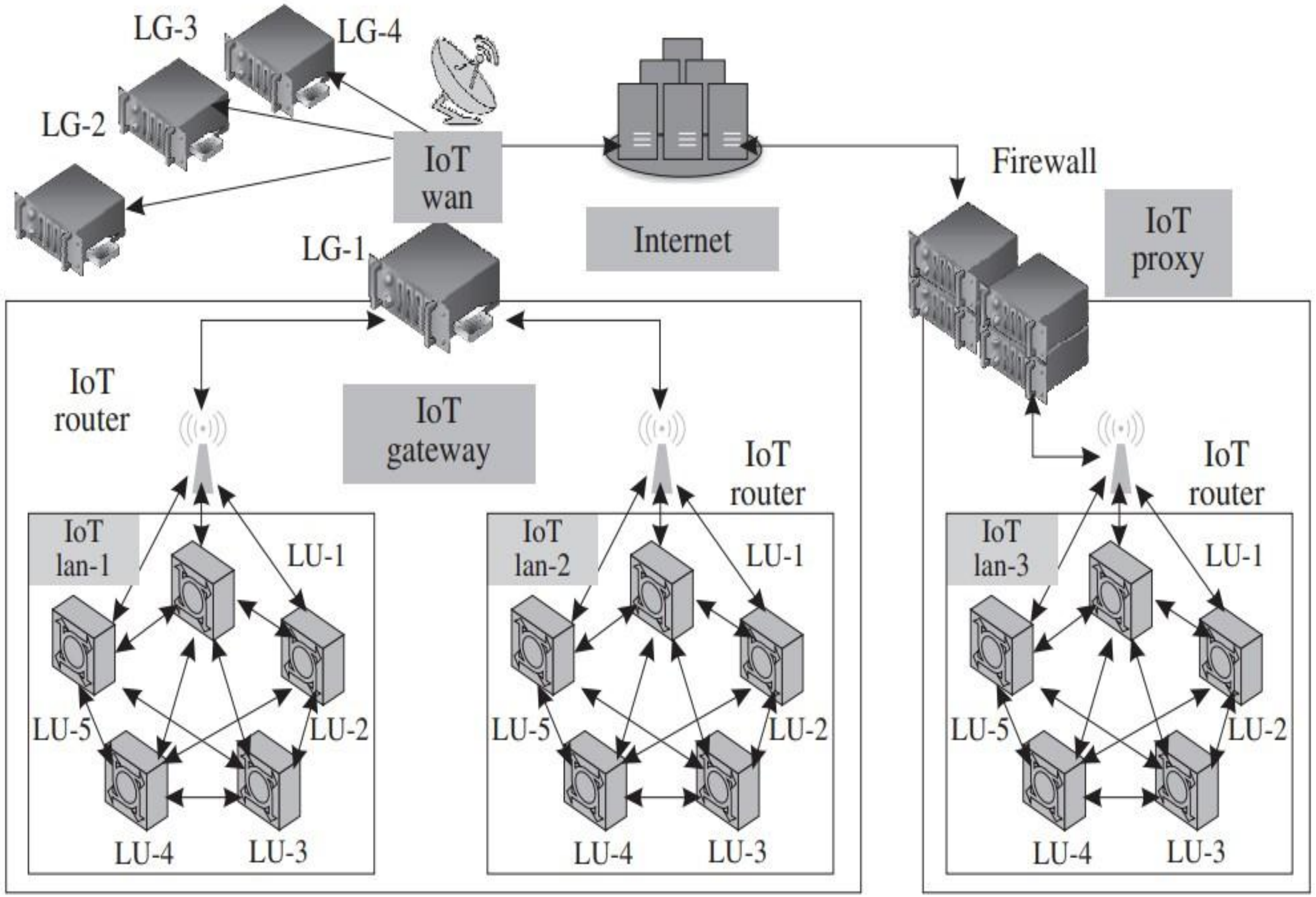


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

6) **IoT proxy:**

- ✓ Proxies actively lie on the application layer and perform application layer functions between IoT nodes and other entities.

- ✓ Typically, the application layer proxies are a means of providing security to the network entities under it; it helps to extend the addressing range of its network.

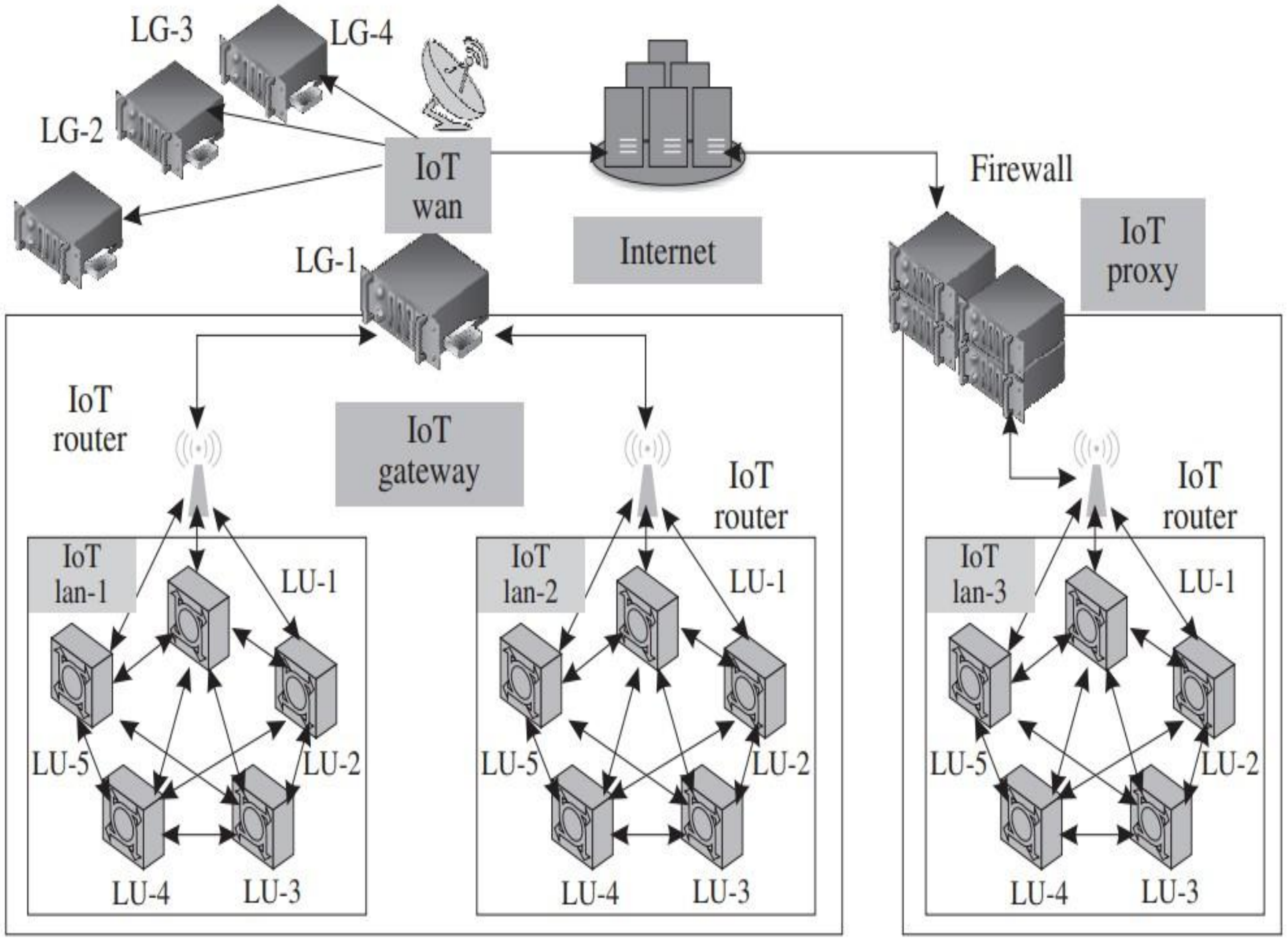


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

IoT Networking Components

The figure summary:

- various **IoT nodes** within an **IoT LAN** are configured to one another as well as talk to the **IoT router** whenever they are **in the range of it**.
- The **devices** have **locally unique (LU-x)** device **identifiers**. These identifiers are unique only within a **LAN**. There is a high chance that these **identifiers** may be **repeated** in a new LAN. **Each IoT LAN has its own unique identifier**, which is denoted by **IoT LAN-x** in Figure.
- A **router** acts as a **connecting link** between various **LANs** by forwarding messages from the **LANs** to the IoT **gateway** or the IoT **proxy**.
- As the **proxy** is an application layer device, it is additionally possible to include **features** such as firewalls, packet filters, and other security measures besides the regular routing operations.
- Various **gateways** connect to an **IoT WAN**, which links these devices to the Internet. There may be cases where the gateway or the proxy may directly connect to the Internet.
- This network may be **wired** or **wireless**; however, IoT deployments heavily rely on wireless solutions. This is mainly attributed to the **large number** of devices that are integrated into the network; **wireless technology** is the only feasible and **neat-enough solution** to avoid the hassles متاعب of laying wires and dealing with the **restricted mobility rising out of wired connections**.

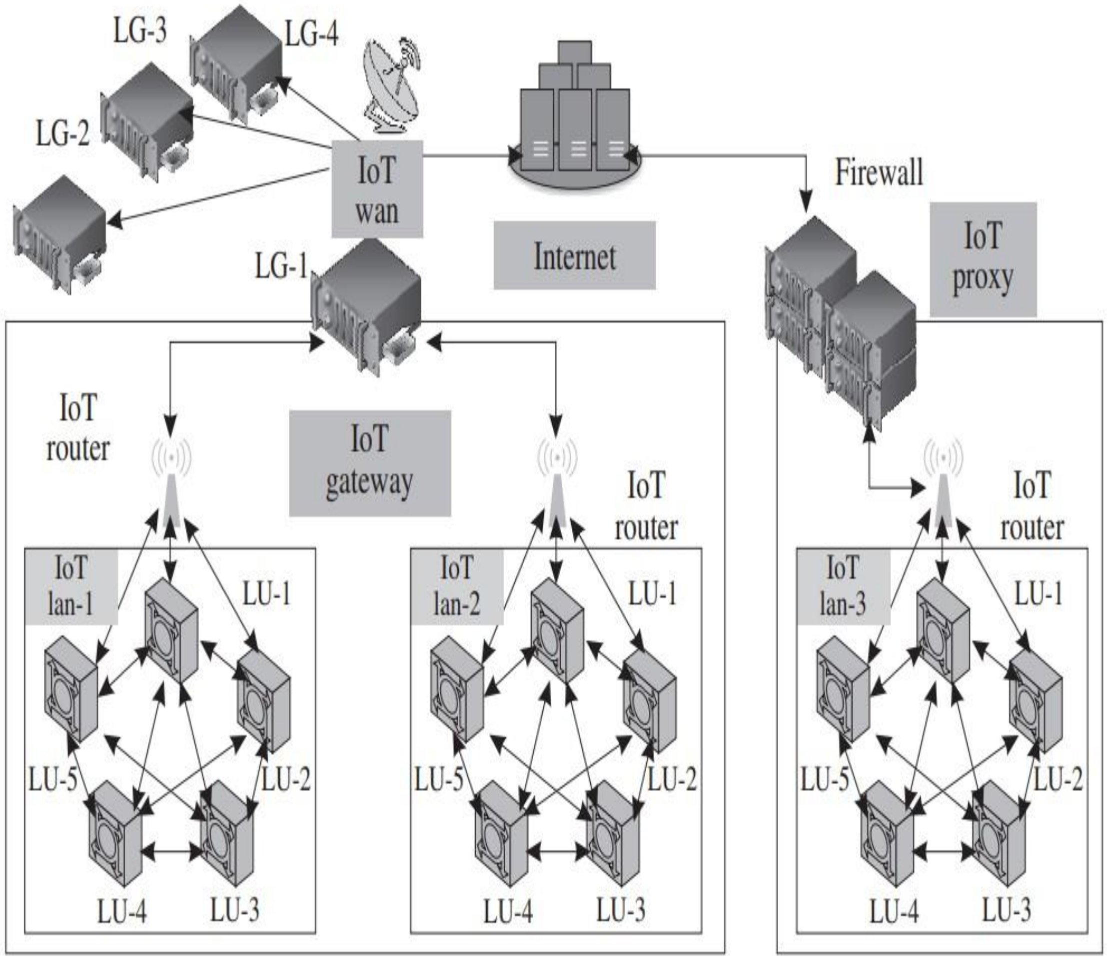
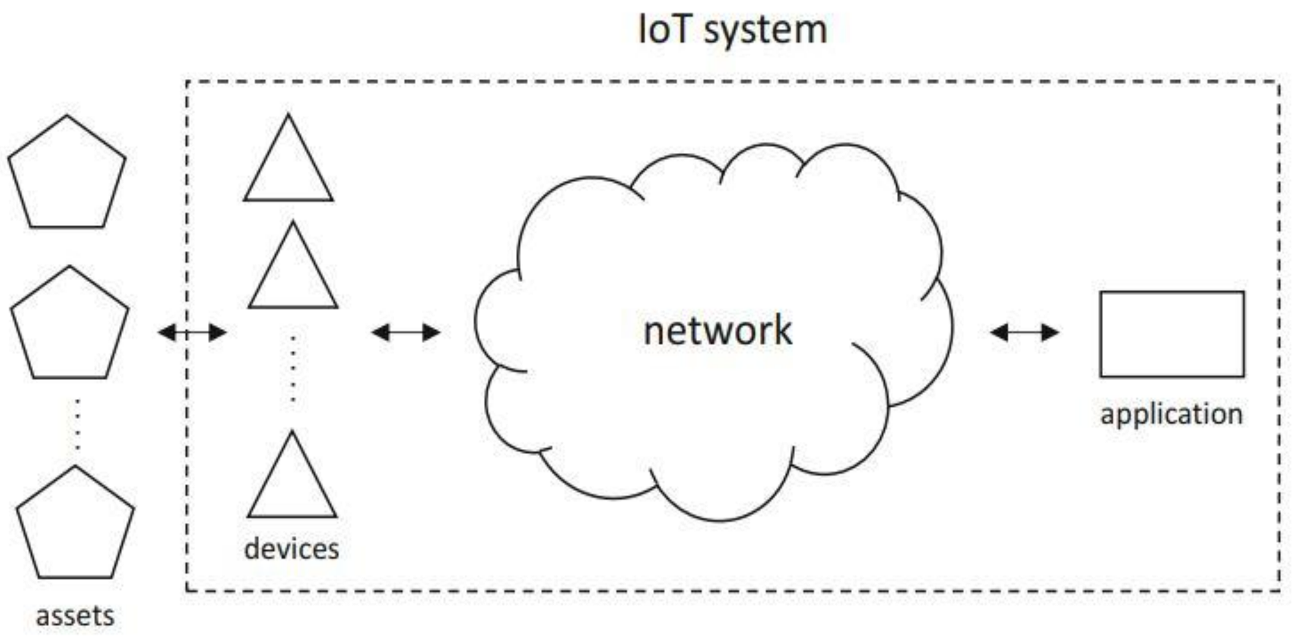
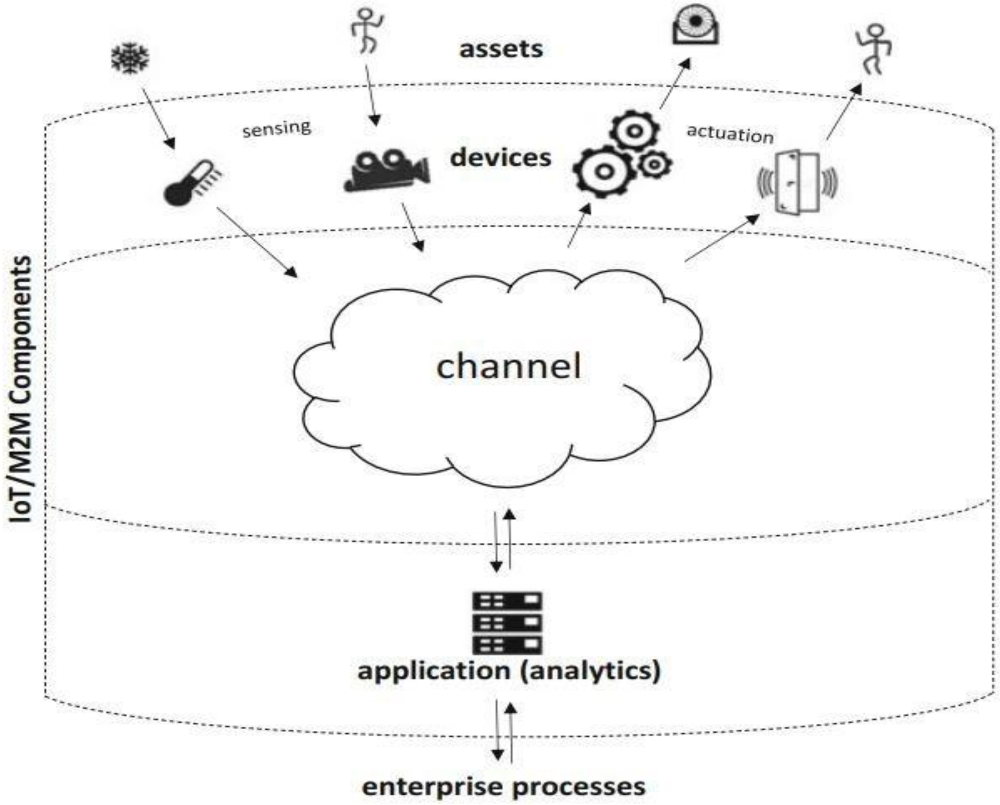


Figure A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

Types of Networks

- **IoT networks** sit in between applications and devices that, in turn, interact with **assets**.
- **The IoT system** is the set made of devices, applications, and networks, while the **asset** is **external** to the **IoT system**.





Types of Networks

- **In the IoT domain**, there are **two** common **scenarios** for communication between **two endpoints**:

  1) one-hop communication (i.e. sensor directly talking to an application)
  2) multi-hop communication (i.e. sensor indirectly talking to an application by relying on intermediate devices to forward packets).

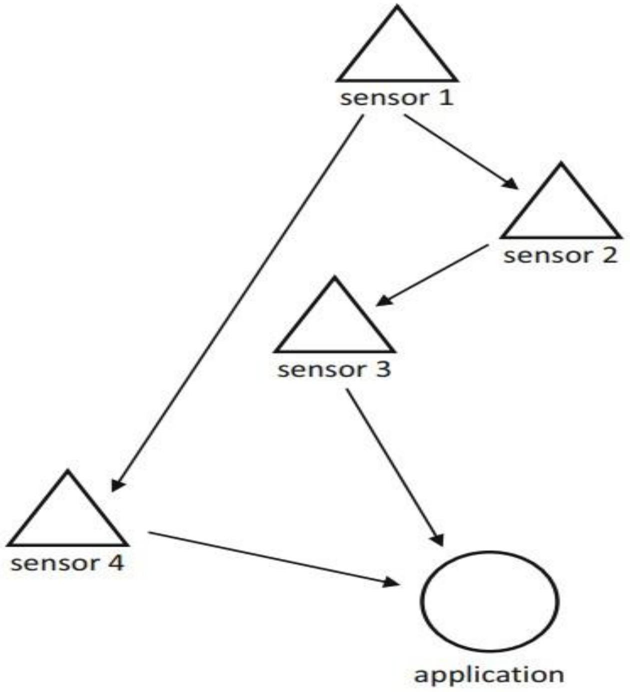


Fig. Multi-hop capillary network

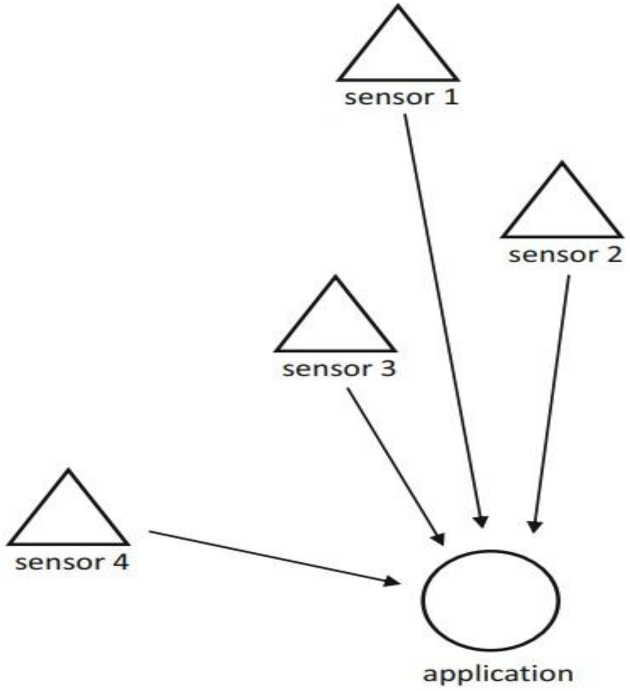
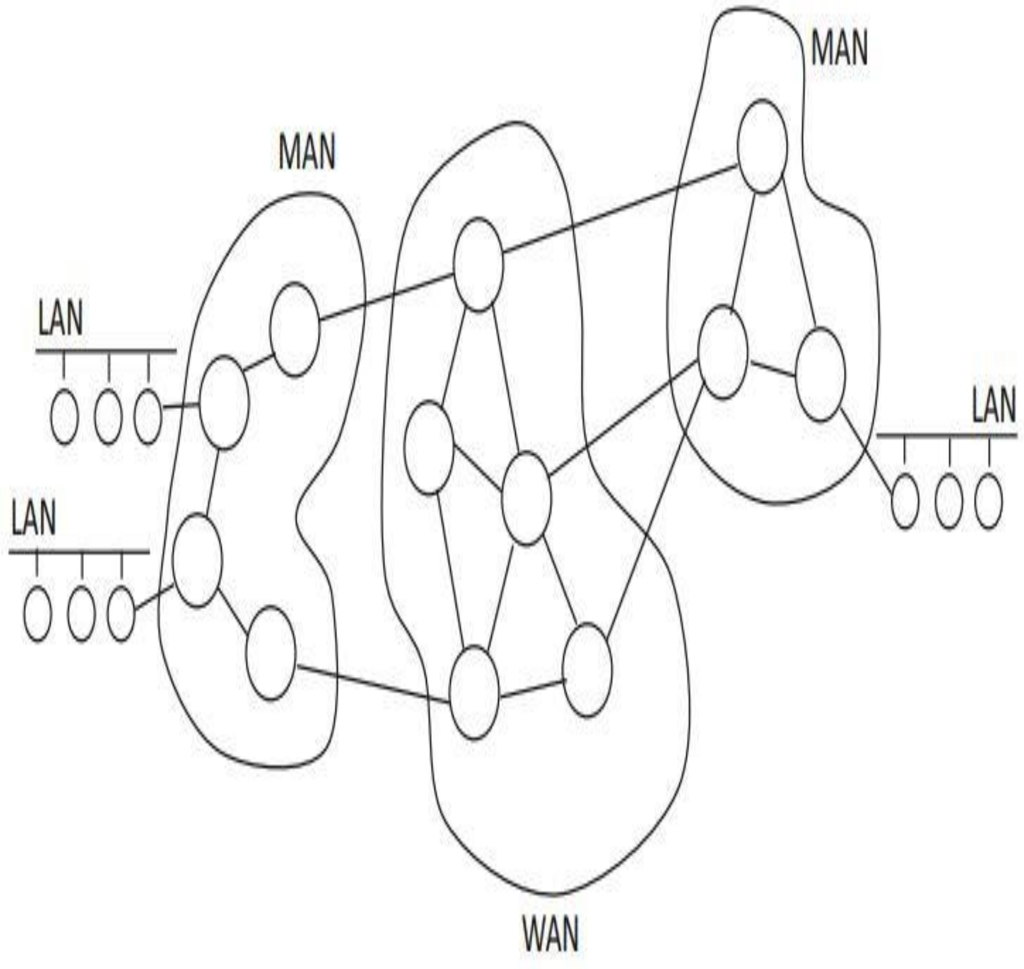


Fig. Single-hop network

Types of Networks

- **Networks** have been **traditionally** classified **based on the area they cover**;
- the **three main types** are local area networks (LANs), metropolitan area networks (MANs), and wide-area networks (WANs).
- A **LAN** **involves** an <u>office</u>, a <u>lab</u>, and a <u>building</u>, and it does not rely on third-party communication infrastructure to provide high-speed service.
- A **WAN**, on the other hand, **involves** a <u>very large geographical</u> region and therefore relies on third-party infrastructure to function. The throughput of a WAN is typically much lower than that of a LAN.
- The size of a **MAN** falls **somewhere** in <u>between that of a LAN and WAN</u>.
- As a WAN, a MAN also relies on third-party communications but operates at higher speeds typically linking LANs and WANs.
- **Larger than WANs**, an Internet area network (IAN) **connects** <u>endpoints within a cloud environment</u>.



Types of Networks

- **Under IoT**, **networking** typically refers to the access network where the devices are located.
- Figure illustrates a **generic IoT access network**.
- In general, the overall **topology** is such that devices interact with an IoT gateway, border router, or cluster head that acts as the **boundary between the access and core sides**.
- The **core network** is usually a mainstream IP network that provides global connectivity to applications.
- These **applications**, in turn, many times reside in the cloud infrastructure.

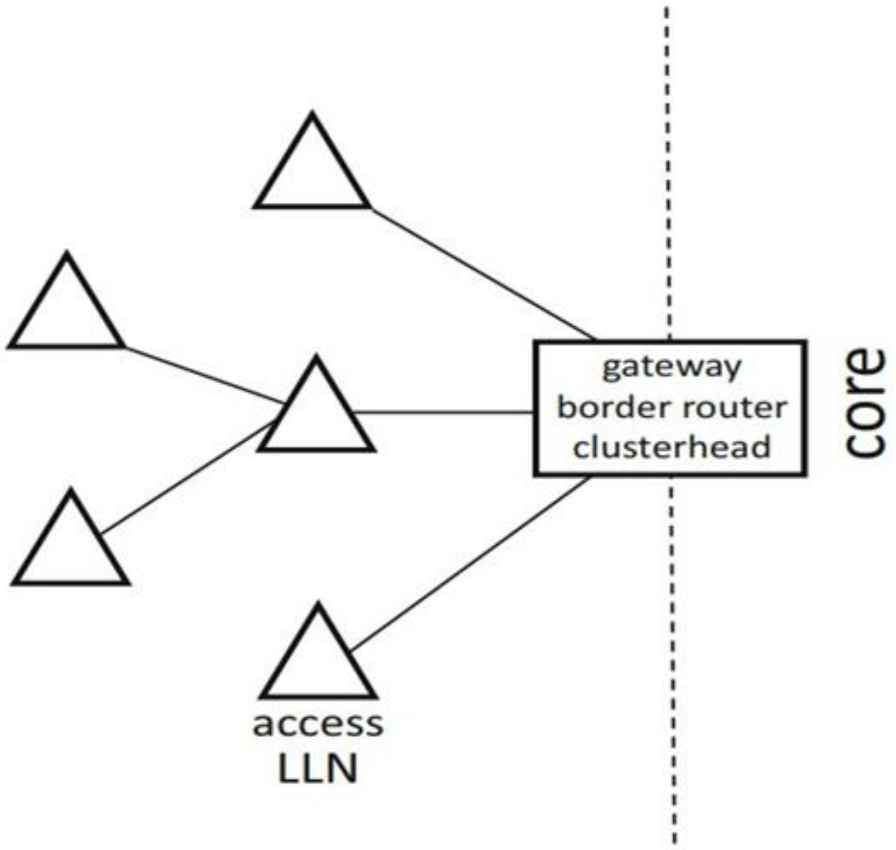
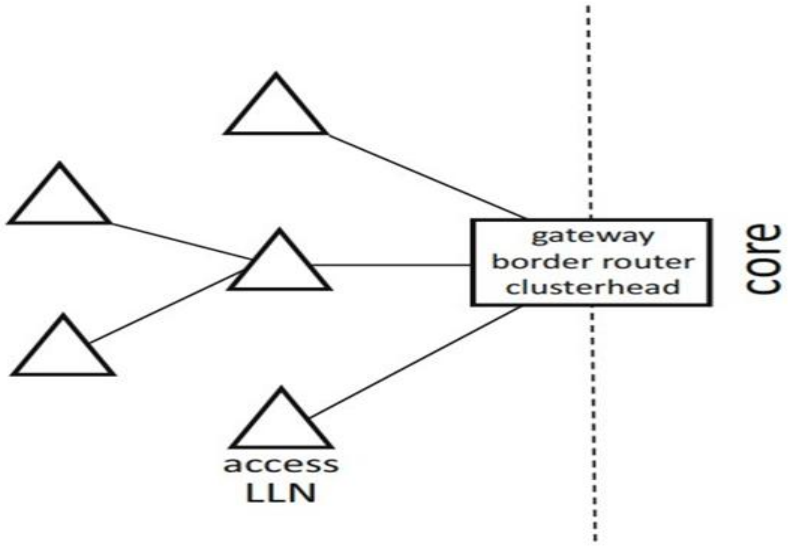
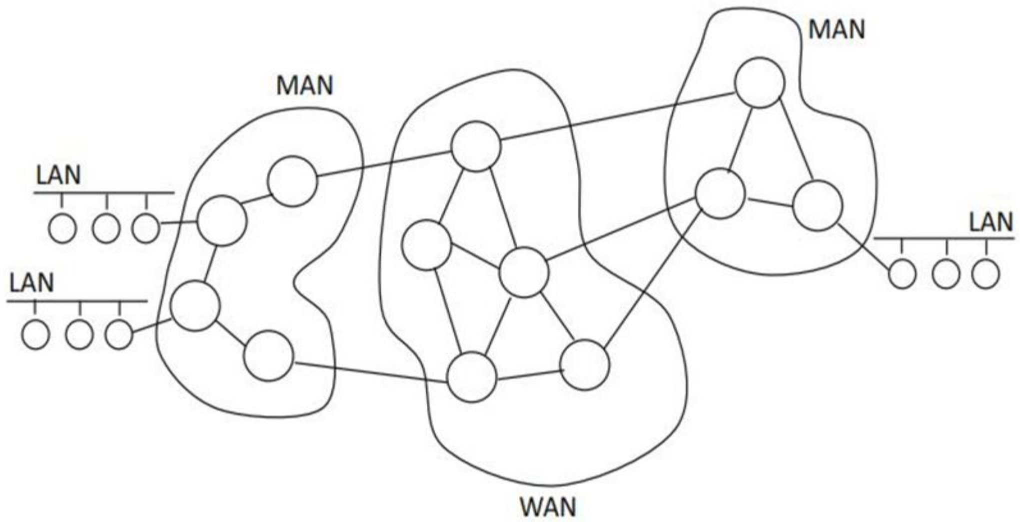


Fig. IoT access network

Types of Networks

- **Most IoT access side networks**, where constrained devices are usually deployed, classify as low-rate short-range LAN subtypes.
- A **home area network (HAN)** is one such subtype that supports IoT communication at home and building levels.
- **Another very popular subtype** that is of particular importance in the **IoT domain** is that of personal area networks (PANs).
- **PANs** provide a small coverage at relatively low transmission rates in order to extend battery life.
- A **very big family of IoT solutions** is based on wireless PANs and therefore called WPANs. **WPANs** are one of the most common network types in the context of IoT.
- With a **smaller coverage than PANs**, body area networks (BANs) are made of wearables and implants as well as other small devices that support fitness and healthcare applications.





Types of Networks

- the **other big family** of IoT networks falls under the WAN umbrella due to their large coverage.

- Because these technologies are **low-power** in order to extend battery life, they are called low-power WANs or LPWANs.

- Note that **although** LPWANs are inherently **wireless**, they are called LPWAN and not LPWWAN.

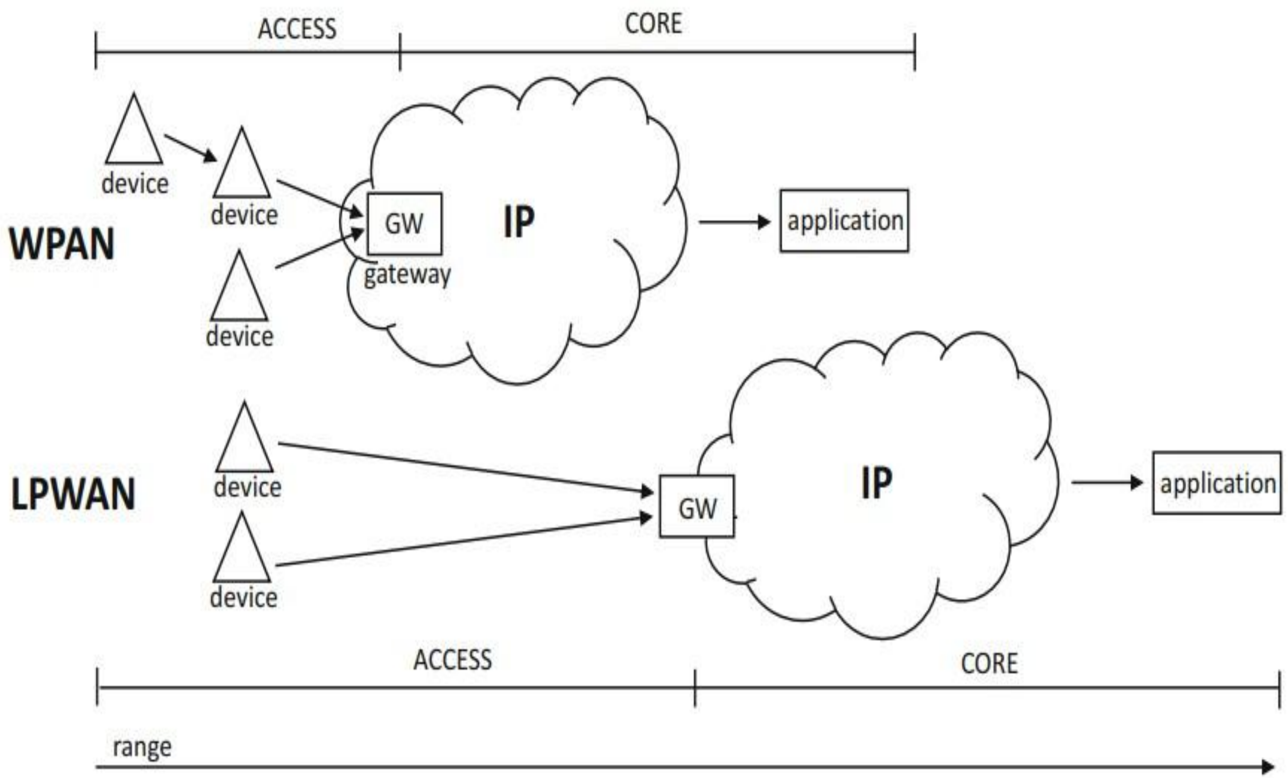
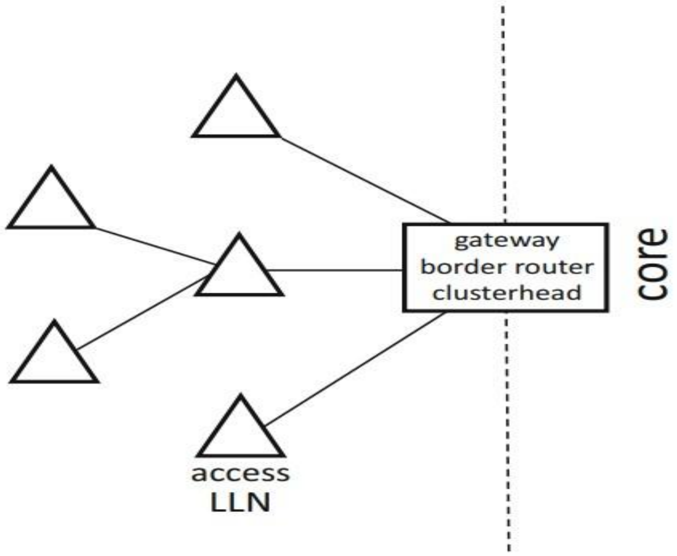
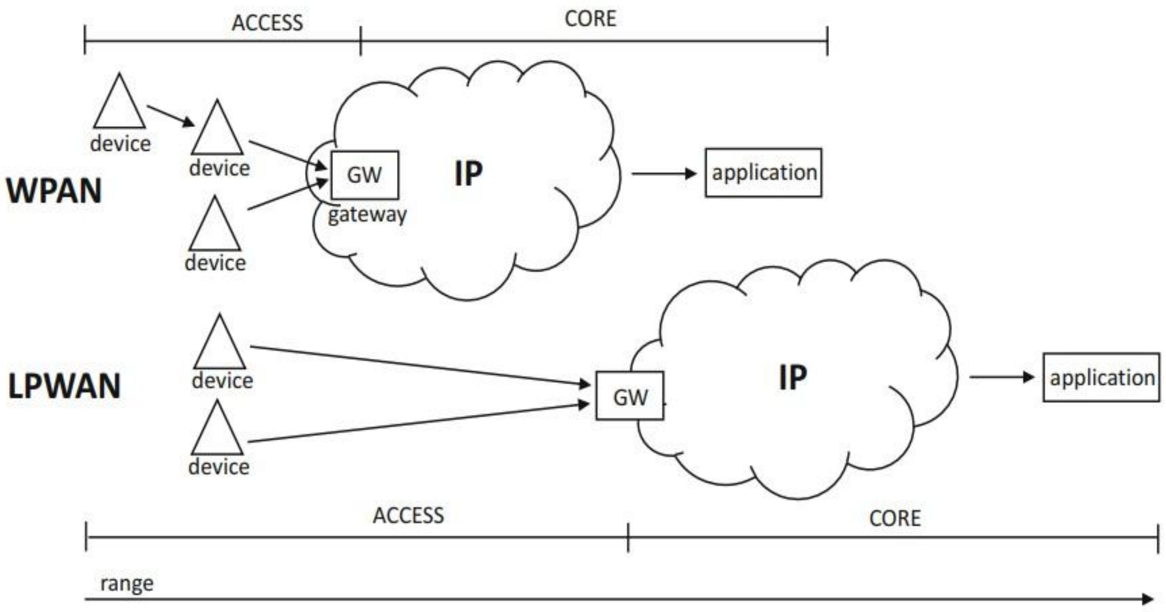


Fig. WPAN vs LPWAN

Types of Networks

- Both **WPANs** and **LPWANs**, by virtue of being wireless, rely on batteries.
- Moreover, **in order to extend battery life**, power consumption must be minimized. **Low power**, unfortunately, implies weak signals and therefore low SNR which is responsible for high packet loss and low transmission rates.
- **Most IoT technologies**, fall under what it is called low-power and lossy networks (LLNs) or are sometimes called low-power, low-rate, and lossy networks (LLLNs).





Devices

- **IoT involves**, by definition, interaction with the physical environment that is performed by means of **logical devices** that can be controllers, actuators, sensors, and gateways. These **logical devices** are supported by hardware provided by physical devices **running on** constrained embedded **computers and systems**.

- They are **constrained** because they have limited memory and computational complexity.

- In general, **these computers** are characterized by a power source, a networking stack, and a processor.

- **The power sources** can be traditional alternating current (AC) and direct current (DC) **electric power lines**, **batteries**, or **hybrid schemes** that support energy harvesting by means of, for example, **solar panels**.

- In regard to **the networking stacks**, and depending on the hardware and software capabilities, there are different protocols associated with layers and technologies as diverse as IEEE 802.15.4 and CoAP.

Devices

- **The processors** are in most cases low-power constrained embedded computers with limited computational complexity and small instruction set architectures (ISAs).

- Because of the IoT interaction with the physical environment, these devices are particularly reliable when it comes to control over timing. Therefore, in many cases, embedded processing is a synonym of real-time processing.

- **The simplest devices** rely on **microprocessors** with **basic central processing units (CPUs)** that combine several peripheral devices like memories, I/O interfaces, and timers. They are usually **8-bit processors** that consume extremely small amounts of energy and rely on power cycles as well as sleep modes to minimize energy consumption and extend battery life. These **small embedded devices** are well known to operate on small batteries for several years.

Devices

- **More advanced devices** rely on **32-bit and 64-bit ARM processors** that comparatively consume more power but provide a lot higher computational complexity including, sometimes, support of digital signal processing (DSP) capabilities.
- Many not-too-complex **embedded processors** rely on co-processors that offload complex functionality like signal and network processing.
- In general, **embedded processors**, regardless of their complexity, include several I/O interfaces that are accessible to system designers by means of pins on System on Chip(SoC) and System on Module (SoM).
- These **interfaces** provide basic communication between **peripherals** within a device by supporting point-to-point and bus infrastructures.

Devices

- **In the context of IoT devices**, **some embedded processors** also include Analog to Digital Converter (ADC) and Digital to Analog Converter (DAC) interfaces for the **conversion of signals** from the analog to the digital and from the digital to the analog domains, respectively.

- Last but not least, **most embedded processors** include general-purpose input and output (GPIO) ports that can be used to read and write two-level digital signals for interaction with sensors and actuators.

- In order to **run complex software**, **complex hardware** is needed. Constrained 8-bit embedded processors are a lot weaker candidates than 64-bit ARM processors to run complex **operating systems (OSs).** Based on levels of complexity, OSs **can be classified** as:

1. main-loop.
2. event-based.
3. Embedded.
4. full-featured.

Devices

1. **main-loop:**

   A main-loop OS consists of a **simple bootloader that executes a single-threaded process** that continuously polls sensors and performs actuation in response.

2. **event-based:**

   An event-based OS is a bit **more sophisticated and relies on hardware interrupts** to report events to an application.

3. **Embedded:**

   An embedded OS, usually called **real-time OS (RTOS),** is lightweight but includes all basic building blocks of traditional OSs including threading, sockets, and contention mechanisms that provide concurrency and real-time functionality.

4. **full-featured:**

   Full-feature OSs, on the other hand, **include all the components and modules** that belong to commercial-grade OSs distributed into kernel and user space elements.

Devices

- In many scenarios, highly constrained devices run as bare-metal devices that do not rely on any OS support, and their firmware provides all functionality.
- the topic of software/hardware interaction and capabilities of embedded devices in the context of IoT is quite complex.
- Based on **hardware** and **software** capabilities, **devices** can be simple or complex.
- **A simple device** relies on a **main-loop** or **event-based** OS running on a battery-powered constrained embedded processor. Examples of simple devices are basic sensors or actuators. Simple device communication is low rate and may or may not rely on IP networking. When a simple device does not natively include an IP interface, Internet connectivity is provided by means of an IoT gateway. Specifically, many simple devices talk to a gateway that converts non-IP into IP traffic. LPWANs are quintessential examples of this scenario.
- **A complex device**, on the other hand, relies on an **RTOS** or on a **full-featured** OS with fully compliant IP stacks. These stacks provide PAN, LAN, and WAN access that provide direct communication to the Internet. Complex devices, such as gateways and stand-alone sensors, rely on **external power** lines that enable **higher transmission rates**.

Devices

- **IoT devices**, and more specifically sensors, controllers, and actuators, can be **self-configured** and **self-organized**.

- **The idea is that** they **can be deployed in a network** such that once they are **powered up**, they can be automatically provisioned and configured to become functional right away.

- **Devices**, at this point, have all the information that enables them to communicate with gateways and applications. **Moreover**, certain devices can also self-propel and support mobility that allows them to deploy themselves in inaccessible remote areas while preserving connectivity.

- **In general**, a highly desired property of IoT devices is **reliability** such that they can operate for years without any human interaction.

Sensors

- **Sensors** are logical devices that sense or measure an asset of the physical environment.
- Examples of assets include **not only physical parameters** like temperature, humidity, and light intensity **but also other measurable quantities** like inventory and population sizes.
- The sensors in each case retrieve temperature, relative humidity, and light intensity as values measured in Centigrade degrees, percentage, and Lux, respectively.
- **Depending on the complexity** of the **embedded processor**, a sensor may perform some local processing in order to remove redundancy in a controlled way.
- An example of this removal is **source encoding** where sensor readouts are digitized and compressed.
- Compression can be **lossless** or **lossy** depending upon whether the original samples can be recovered or not.
- Specifically, through **source encoding**, data is converted into information that can be transmitted at lower rates reducing the channel bandwidth requirements and improving power consumption.

Sensors Classify

- The various sensors can be classified based on:

1) **power requirement**,
2) **Sensor output**,
3) **property to be measured**.

Sensors Classify

1) power requirement,

The way sensors operate decides the power requirements that must be provided for an IoT implementation. Some sensors need to be **provided with separate power sources** for them to function, whereas some sensors **do not require any power sources**. Depending on the requirements of power, sensors can be of two types.

(i) **Active:** Active sensors **do not require** external circuitry or mechanism to provide them with power. It directly responds to the external stimuli from its ambient environment and converts them into an output signal. **For example**, a photodiode converts light into electrical impulses.

(ii) **Passive:** Passive sensors **require** an external mechanism to **power** them up. The sensed properties are modulated with the sensor's inherent characteristics to generate patterns in the output of the sensor. **For example**, a thermistor's resistance can be detected by applying voltage difference across it or passing a current through it.

Sensors Classify

2) Sensor output:

The output of a sensor helps in deciding the additional components to be integrated with an IoT node or system. Typically, almost all modern-day processors are digital; **digital sensors** can be directly integrated to the processors. However, the integration of **analog sensors** to these digital processors or IoT nodes requires additional interfacing mechanisms such as **analog-to-digital converters (ADC),** voltage level converters, and others. Sensors are broadly divided into two types, depending on the type of output generated from these sensors, as follows.

(i) Analog.

(ii) Digital.

Sensors Classify

2) Sensor output:

i. **Analog**: Analog sensors **generate an output signal or voltage**, which is proportional (linearly or non-linearly) to the quantity being measured and is continuous in time and amplitude. Physical quantities such as temperature, speed, pressure, displacement, strain, and others are all continuous and categorized as analog quantities. For example, a thermometer or a thermocouple can be used for measuring the temperature of a liquid (e.g., in household water heaters). These sensors continuously respond to changes in the temperature of the liquid.

ii. **Digital**: These sensors **generate the output of discrete time digital representation** (time, or amplitude, or both) of a quantity being measured, in the form of output signals or voltages. Typically, binary output signals in the form of a logic 1 or a logic 0 for ON or OFF, respectively are associated with digital sensors. The generated discrete (non-continuous) values may be output as a single "bit" (serial transmission), eight of which combine to produce a single "byte" output (parallel transmission) in digital sensors.

Sensors Classify

3) property to be measured:

The property of the environment being measured by the sensors can be crucial in deciding the number of sensors in an IoT implementation. **Some properties** to be measured do not show high spatial variations and can be quantified **only based on** temporal variations in the measured property, such as ambient temperature, atmospheric pressure, and others. **Whereas some** properties to be measured show high spatial **as well as** temporal variations such as sound, image, and others. Depending on the properties to be measured, sensors can be of two types.

i. Scalar.

ii. Vector.

Sensors Classify

3) property to be measured:

i. **Scalar**: Scalar sensors produce an output proportional to the magnitude of the quantity being measured. The output is in the form of a signal or voltage. Scalar physical quantities are those where only the magnitude of the signal is sufficient for describing or characterizing the phenomenon and information generation. **Examples** of such measurable physical quantities include color, pressure, temperature, strain, and others. A thermometer or thermocouple is an example of a scalar sensor that has the ability to detect changes in ambient or object temperatures (depending on the sensor's configuration). Factors such as changes in sensor orientation or direction do not affect these sensors (typically).

ii. **Vector**: Vector sensors are **affected** by the magnitude as well as the direction and/or orientation of the property they are measuring. Physical quantities such as speed and images that require additional information besides their magnitude for completely categorizing a physical phenomenon are categorized as vector quantities. Measuring such quantities are undertaken using vector sensors. For example, an electronic gyroscope, which is commonly found in all modern aircraft, is used for detecting the changes in orientation of the gyroscope with respect to the Earth's orientation along all three axes.

Sensors

- **Battery life can be extended** by means of **power duty cycles** where devices **sleep** by dramatically reducing power consumption at preprogrammed intervals.
- Specifically, **while a device sleeps**, it minimizes power consumption by **only enabling basic functionality** including a wake-up interrupt or notification.
- In order to minimize network throughput and preserve the power consumption of all devices to extend the network lifetime, it is preferable that duty cycles are **coordinated** throughout the network.
- This is particularly **important** when considering capillary networks that rely **on multi-hop communication** where intermediate sensors act as routers.
- **If a sensor does not know whether transitional devices are sleeping** at any given time, it may waste energy to transmit data to an **inactive router** that is not able to propagate packets to a destination.

Sensors

- **From a networking perspective**, depending on the use of **the sensor readouts**, transmission reliability is important.

- If sensor readouts are to be **used to make real-time decisions** like changing the flight path of a UAV, latency, and packet loss must be as low as possible.

- On the other hand, **if those readouts are to be used to perform offline data visualization**, latency, and packet loss requirements are a lot less restrictive.

- In general, **application-specific quality of service QoS** goals lead to different application latency and packet loss levels that tell how reliable sensor data transmission must be.

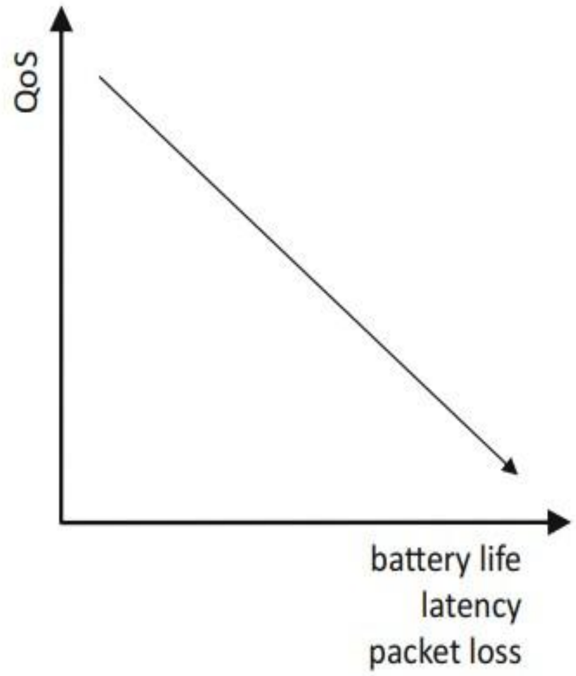


Fig. QoS vs battery life, loss, and latency

Actuators and Controllers

- **Actuators** are logical devices that **perform some external change of an asset of the physical environment**.
- An example of actuation is the activation of a **fan** to **lower the temperature of a room**. In this case, the **actuator** is the fan, and the **asset** is the temperature.
- Another example of actuation is the servos that can be used to change the flight path of a UAV. Similarly, the servos are the actuators, and the flight path is the asset.
- Actuation is typically tied to sensing through feedback mechanisms where decision-making takes sensor and actuation data as input and output parameters, respectively.
- Because of this, if a given physical device has a logical actuator, it is quite likely that a logical sensor is also present. **The opposite**, that is, the presence of an actuator given a sensor is present, is a **lot less common**.
- Same way sensors are associated with source encoding and DACs, actuators are associated with source decoding and ADCs. Actuators, however, are a lot simpler as they do not rely on data-information and information-knowledge conversions. Usually the knowledge from the application results in a command being sent down to the actuator. As with sensors, actuators are affected by loss and latency that results in different QoS levels.

Actuators and Controllers

- **Controllers** are logical devices that **perform some internal change in the physical device** to assist sensing or actuation.

- This involves, **for example**, having a camera zoom in and out, replacing optical filters, or having a transmitter turn antennas around.

- In most cases, **controllers are deployed along with sensors and actuators** as logical devices on the same physical device. When assisting sensing, control is affected by the same application QoS requirements that are needed by the sensor.

Gateways

- **Gateways** are logical devices that serve as an interface between access-side IoT devices and core-side applications.
- **Access side IoT** devices are the sensors, actuators, and controllers, while the **core side applications** rely on analytics to make real-time decisions.
- **When compared to other devices**, the gateway is a bit more advanced, demanding higher computational complexity that requires more resourceful and powerful embedded processors fed by power lines.
- **This complexity** is also needed for the gateway to have enough “horsepower” to simultaneously interact with multiple sensors, actuators, and controllers.
- This does not prevent, **in certain scenarios** typically associated with multi-hop communications, simpler devices like sensors **and** actuators from providing basic gateway functionality.

Gateways

- Specifically, **sometimes networks can rely on sensors and actuators** taking turns in becoming temporary gateways that aggregate and forward packets to uplink applications. Of course, this is contingent on device’s computational complexity and battery life.

- Many times, **gateways** are critical in providing communication between devices, as they route all traffic up and down the network. This is especially true when the gateway acts as cluster heads that forward back and forth all packets on the access side.

Gateways

- **In most IoT scenarios**, **gateways** are known to provide interfaces between WPANs and LPWANs on the access side and mainstream WANs on the core side.
- In a more generic definition, **gateways** translate messages at different levels of the layered architecture.
- **They can: (1)** convert physical and link layer frames, for example, when forwarding them between wireline Ethernet and wireless IEEE 802.15.4;
- **they can (2)** convert network layer datagrams, for example, when forwarding them between IPv4 and 6LoWPAN/IPv6 layers;
- **they can (3)** convert transport layer segments, for example, when forwarding them between Transport Control Protocol (TCP) and UDP layers; and
- **they can (4)** convert application layer messages, for example, when forwarding them between Hypertext Transfer Protocol (HTTP) [1] and CoAP layers. Table 2.1 compares gateways against the other devices regarding computational complexity, networking capabilities, and hardware form factors.

Table Device comparison

Device	Complexity	Networking	Form factor
Sensor	Low	WPAN/LPWAN	Small
Actuator	Low	WPAN/LPWAN	Medium
Controller	Low	WPAN/LPWAN	Medium
Gateway	High	WPAN/LPWAN WAN	+Large

Acknowledgment

- **These lecture slides are based on:**

1) **Chapter 3 (P 87-88)** from the book "Introduction to IoT" by (Sudip Misra, Anandarup Mukherjee, Arijit Roy).
2) **Chapter 2 (P 21-29)** "Fundamentals of IoT Communication Technologies" by (Rolando Herrero)

Basics of Networking

END OF LECTURE (4)

Keep connected with the classroom

btukscx

THANK YOU FOR YOUR ATTENTION