INSTITUCIÓN UNIVERSITARIA DE ENVIGADO
Ciencia , educación y desarrollo
Vigilada Mineducación

IoT – Network Types and Architectures

Prof. Jaime A. Riascos

Internet-of-Things

University Institution of Envigado (Colombia)

2022

Introduction

- Imagine that one day you decide to build a house.
- To successfully complete a construction project, time and effort are required to design each phase, from the foundation to the roof.
- Your plans must include detailed designs for the electrical, plumbing, heating, and security systems.

Introduction

- A computer network should be built with-- careful planning, security policies, and adherence to well-understood design practices.

- Failure to meet these will likely result in something that is difficult to scale, manage, adapt to organizational changes, and, worst of all, troubleshoot when things go wrong

- If the network fails, company operations can be seriously impaired

Introduction

- Just as a house must be designed with the strength to withstand potential natural disasters, such as seismic events and hurricanes,

- Information technology (IT) systems need to be designed to withstand "network earthquakes," such as:
  - distributed denial of service (DDoS) attacks,
  - future growth requirements,
  - network outages, and
  - even human error

Drivers Behind New Network Architectures

Building residential houses vs building a massive stadium…

- The difference between IT and IoT networks is much like the difference between residential architecture and stadium architecture
- The key difference between IT and IoT is the data.
- IT systems are mostly concerned with the reliable and continuous support of business applications such as email, web, databases, CRM systems, and so on.
- IoT is all about the data generated by sensors and how that data is used
- The essence of IoT architectures thus involves how the data is transported, collected, analyzed, and ultimately acted upon

Security

- IT networks use firewall, IT endpoints are behind a firewall
- IoT endpoints are often located in wireless sensor networks that use unlicensed spectrum and are not only visible to the world through a spectrum analyzer but often physically accessible
- IoT systems require consistent mechanisms of authentication, encryption, and intrusion prevention techniques.

IoT systems must:

- Be able to identify and authenticate all entities involved in the IoT service (that is, gateways, endpoint devices, home networks, roaming networks, service platforms)
- Ensure that all user data shared between the endpoint device and back-end applications is encrypted
- Comply with local data protection legislation so that all data is protected and stored correctly
- Take network-level approach to security in addition to device level approach

Constrained Devices and Networks

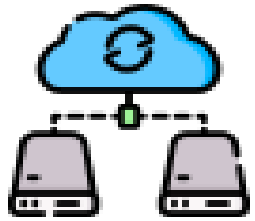
- Most IoT sensors are designed for a single job, and they are typically small and inexpensive
- They often have limited power, CPU, and memory, and they transmit only when there is something important
- The networks that provide connectivity also tend to be very lossy and support very low data rates.
- This is a completely different situation from IT networks
- IoT requires a new breed of connectivity technologies that meet both the scale and constraint limitations

Legacy Device Support

- Supporting legacy devices in an IT organization is not usually a big problem
- If someone's computer or operating system is outdated, she simply upgrades
- If someone is using a mobile device with an outdated Wi-Fi standard, such as 802.11b or 802.11g, you can simply deny him access to the wireless network, and he will be forced to upgrade
- In OT systems, end devices are likely to be on the network for a very long time—sometimes decades.
- As IoT networks are deployed, they need to support the older devices already present on the network, as well as devices with new capabilities

IoT Network

Networking technologies enable IoT devices to communicate with other devices, applications, and services running in the cloud.



The internet relies on standardized protocols to ensure communication between heterogeneous devices is secure and reliable.

Standard protocols specify rules and formats that devices use to establish and manage networks and transmit data across those networks.

IoT Network

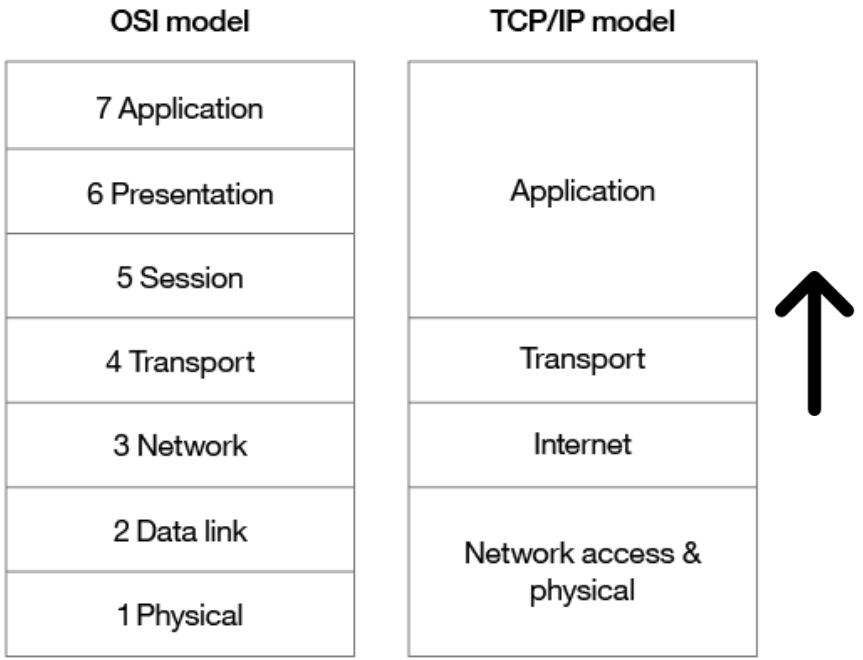
- Networks are built as a “stack” of technologies.
- A technology such as Bluetooth LE is at the bottom of the stack. While others such as such as IPv6 technologies (which is responsible for the logical device addressing and routing of network traffic) are further up the stack.
- Technologies at the top of the stack are used by the applications that are running on top of those layers, such as message queuing technologies.

Networking standards and technologies

The networking protocols and specific technologies that implement each protocol are assembled in layers with a specific function.

The Open Systems Interconnection (OSI) model is a standard abstract model of seven protocol layers, whose order is from down to top presented in the table below.

TCP/IP provides a simplified concrete implementation of these layers in the OSI model.



OSI and TCP/IP networking models

Network Access & Physical Layer

This TCP/IP Layer subsumes both OSI layers 1 and 2. The physical (PHY) layer (Layer 1 of OSI) governs how each device is physically connected to the network with hardware, for example with an optic cable, wires, or radio in the case of a wireless network like wifi IEEE 802.11 a/b/g/n).

At the link layer (Layer 2 of OSI), devices are identified by a MAC address, and protocols at this level are concerned with physical addressing, such as how switches deliver frames to devices on the network.

Internet Layer

This layer maps to the OSI Layer 3 (network layer). OSI Layer 3 relates to logical addressing. Protocols at this layer define how routers deliver packets of data between source and destination hosts identified by IP addresses.

IPv6 is commonly adopted for IoT device addressing.

Transport Layer

The transport layer (Layer 4 in OSI) focuses on end-to-end communication and provides features such as reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent.

UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.

Application Layer

The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging.

HTTP/S is an example of an application layer protocol that is widely adopted across the internet.

IoT network

Although the TCP/IP and OSI models provide you with useful abstractions for discussing networking protocols and specific technologies that implement each protocol, some protocols don’t fit neatly into these layered models and are impractical.

For example, the Transport Layer Security (TLS) protocol that implements encryption to ensure privacy and data integrity of network traffic can be considered to operate across OSI layers 4, 5, and 6.

IoT networking protocols

The networking protocols are adopted in IoT fitting the TCP/IP layers that are applied using the same concept.

The structure of a network (topology) and other concepts are that change.

Commonly are used star and mesh topologies. In star topology, each IoT device is directly connected to a central hub (gateway). In a mesh topology, the devices connect to other devices within range of each node route traffic as can gateway nodes. Then, each one communicates with data from the connected devices upstream.

Each layer is adapted to IoT Protocols.

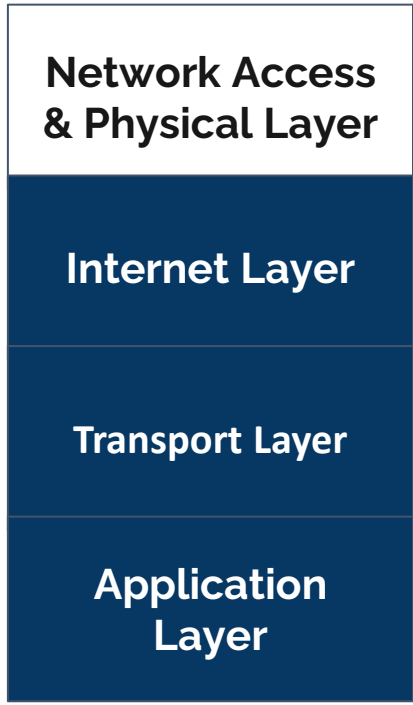
TCP/IP model	IoT protocols
Application	HTTPS, XMPP, CoAP, MQTT, AMQP
Transport	UDP, TCP
Internet	IPv6, 6LoWPAN, RPL
Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE

IoT network protocols mapped to the TCP/IP model

IoT networking protocols

This Layer Focus on how each device is physically connected to the network with hardware.

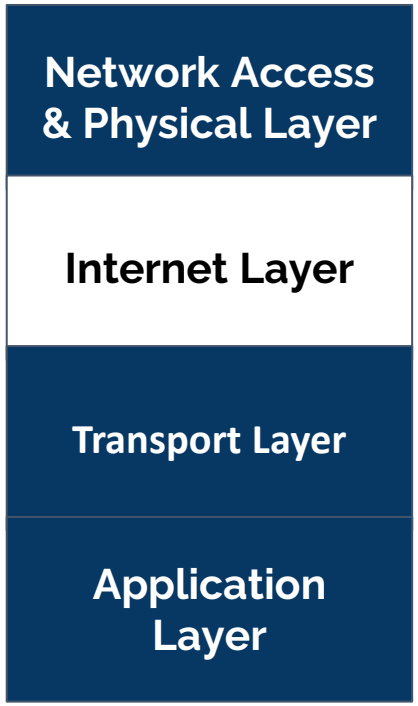
- **LPWAN:** Low Power Wide Area Network, for **low-power, long-range** wireless communication. Devices as **LoRa** and others.
- **Cellular:** Allow **low-power, low-cost** IoT communication options using existing cellular networks, is focused on long-range communication between large numbers of primarily indoor devices.
- **BLE: Bluetooth Low Energy**, is a **low-power** version of the popular Bluetooth 2.4 GHz wireless communication protocol, for **short-range** communication and **save power** when they are not transmitting data.
- **NFC:** The **near field communication** protocol, is used for **very small range communication** (up to 4 cm), such as holding an NFC card or tag next to a reader.
- **Wifi:** Wifi is standard **wireless networking** that offers the **highest data throughput**, but at the cost of **high-power consumption**, it is likely that wifi will be superseded by lower-power alternatives.
- **Ethernet:** Widely deployed for **wired connectivity** within local area networks, devices need to be **stationery wireless.**



IoT networking protocols

This Layer is used to define the deliver packets of data between source and destination, are used some such as:

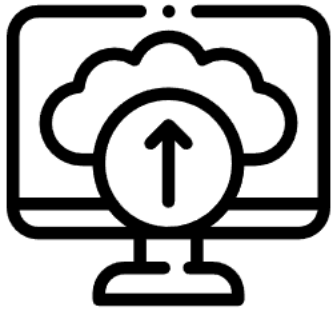
- **IPv6:** IPv6 is typically used for IoT applications to provides 2^128 addresses (around 3.4 × 10 38 or 340 billion billion billion billion)
- **6LoWPAN:** The **IPv6 Low Power Wireless Personal Area Network (6LoWPAN)** allows IPv6 to be used for wireless sensor networks, and others.
- **RPL:** The **IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is designed for routing IPv6 traffic over low-power networks** like those networks implemented over 6LoWPAN, but is designed for routing packets **within constrained networks.**



IoT networking protocols

The transport layer focuses on end-to-end communication and provides features such as **reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order** that they were sent.

UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.



IoT networking protocols

This Layer is used to covers application messaging to activate any intern functionality:

- **MQTT: Message Queue Telemetry Transport,** is a publish/subscribe-based messaging protocol for low bandwidth situations.
- **AMQP: Advanced Message Queuing Protocol,** is an open standard messaging protocol that is used for message-oriented middleware.
- **XMPP: The Extensible Messaging and Presence Protocol,** for machine-to-machine (M2M) communication to implement lightweight middleware.

Network Access & Physical Layer
Internet Layer
Transport Layer
Application Layer

IoT networking considerations and challenges

When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:

- **Range**
- **Bandwidth**
- **Power Usage**
- **Intermittent Connectivity**
- **Interoperability**
- **Security.**

IoT networking considerations and challenges

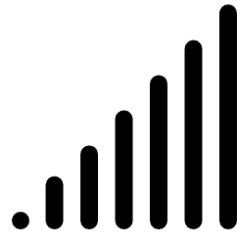
Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network. **Select a network protocol that matches the range that is required:**

- **PAN (Personal Area Network): Short range** in meters, such as Bluetooth BLE.
- **MAN (Metropolitan Area Network): Long Range** (city wide), in few kilometers, such as smart parking sensors installed throughout a city.
- **LAN (Local Area Network): Short to Medium range,** in hundreds of meters, such as Interconnections in the same building.
- **WAN (Wide Area Network): Long range,** in kilometers, such as agricultural sensors that are installed across a large farm.

IoT networking considerations and challenges

Bandwidth is the amount of data that can be transmitted per unit of time. It limits the rate at which data can be collected from IoT devices and transmitted upstream. Bandwidth is **affected by many factors**, which include:

- **The volume of data each device gathers and transmits.**
- **The number of devices deployed.**
- **Whether data is being sent as a constant stream or in intermittent bursts, and if any peak periods are notable.**



This mainly affects the latency time of the data.

IoT networking considerations and challenges

Power Usage

Transmitting data from a device consumes power and its proportional to the distance. You must consider the power source with their total lifecycle to provide greater reliability and optimization of this such as sleep mode or modeling the energy consumption

Intermittent Connectivity

Designs should incorporate intermittent connectivity and seek any available solutions to provide uninterrupted service to avoid interferences or disconnections or consider periodical connections..

Interoperability

The many **different designs and variability of characteristics** into the IoT devices mu**st be allows into the network connections and avoid incompatibility** issues, to work in a more robust way

IoT networking considerations and challenges

Based on **IEEE 802.15.4** security model provides:

- Access Control
- Message Integrity
- Message Confidentiality
- Replay Protection

Consider the **following factors** in a **secure IoT network:**

- **Authentication:** Ensures to **access control** to certain resources, such with the user login. Consider **based on X.509** standard for device authentication.

Security

It is a Priority

- **Encryption:** Ensures **message integrity and confidentiality** with the use of **TLS or DTLS (Transport Layer Security)** that encrypts application data. For example in WiFi, use **Wireless Protected Access 2 (WPA2)** or **Private Pre-Shared Key (PPSK)** approach.

Conclusions

- **Selected networking technologies** will impact the design of IoT devices. The considerations suggested in this article **depend on many factors**. For example, **network range, data rate, and power consumption** are all directly related.

- For **basic home automation**, Bandwidth limitations and drop-outs in connectivity are priorities and aren't the power consumption. **WiFi is not optimized for low-power devices**, making it an unwise choice for a battery-powered device.

- This article provides an overview of s**ome of the most common networking protocols and technologies for IoT**. **It is most important** the IoT networking challenges to **find the technologies that will be the best fit for your IoT application.**

Thank you

Questions?

Refs:

https://mite.ac.in/wp-content/uploads/2021/04/iot_module1.pdf

Gerber, A. & Romeo, J. (2020, Enero). Connecting all Things in the Internet of Things. IBM. **https://developer.ibm.com/articles/iot-lp101-connectivity-network-protocols/**