CS 498: Internet of Things

Chufan Chen

November 10, 2021

"A good stock of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one."

– Paul Halmos.

"Constrained optimization is the art of compromise between conflicting objectives."

– William A. Dembski.

Contents

1 Week 1 Lectures: Computer Internetworking

1.1 Week 1 Overview

The Internet of Things is amazing, but it's not like it's some completely new thing. The amazing devices and technologies being are made up of systems, protocols, and architectures that have been around for decades. So in order to understand IoT, it's important to understand some key pieces of the Internet.

In this week, we'll talk about the Internet, including how it works; how it is designed, its key protocols, and underlying services. We will also describe two example use cases and applications of IoT, some of the challenges they present, and mention how Internet technologies can be applied to solve these problems. After you get through these lectures, you'll have a good basic understanding of the Internet, which will serve as a strong foundation towards understanding the designs and architectures of IoT. Internet Architecture: Domain Name System (DNS), IP addresses, IP prefixes, Routing Tables, Router Interfaces, Ethernet, Inter- and Intra-domain routing, VLANs; Delivery models: Unicast/Broadcast/Multicast/Anycast.

Key Phrase/Concepts

- OSI/TCP Stacks; 7-Layer model: Application, Presentation, Session, Transport, Networking, Datalink (MAC), Physical.
- IoT Protocols: Bluetooth, Bluetooth Low Energy (BLE), Zigbee, WiFi Halow, LoRa, LTE-M, NB-IoT.
- IoT Applications: Environmental monitoring, Smart homes/buildings/cities.

1.2 Background: How the Internet Works

1. Internet Architecture
2. Networking Routing
3. Network Devices

How Can Two Hosts Communicate?

Connect these hosts together witgh a wire, and then we can modulate properties of this wire to send information. We can take text, or images, or video, and encode it in series of ones and zeros, and then we can encode those ones and zeros as voltage changes on the wire. We can seem a high voltage for a one, a low voltage for a zero. So we can send pulses of electricity over the wire, and the other site can decode the message by receiving these pulses and figure out if the other side is sending a one or a zero. Now it turns out, this isn't the most efficient way to send information. We can send pulses for ones and no pulses for zeros to send information, we could do that. But it turns out due to certain reasons and we'll get into these reasons later, it's more efficient to send a continuous signal called a **carrier signal**, a continuous sine wave and then very properties of that sine wave to send information. So in particular, we can change the phase or the frequency of their amplitude, properties of that sine wave signal to send information. By doing this, we can get higher bandwidths and this is how real protocols work. We can send signals over copper, over some conductor, we can also make wires that transmit light. We can actually send pulses of light to send information that's called the optical cable. We can use air which is wireless.

How Can Many Hosts Communicate?

Naive apporach: Full mesh, This is a topology where all pairs of hosts are interconnected. Problem: Full mesh do exist in the Internet. There are certain places where you need very tight coupling inside of data centers or ISPs, you need a lot of resilience. Those are the cases were you use full mesh topologies, but there's no way you would use it in the white area to build the entire Internet, is **not very scalable**. Better approach: Multiplex traffic with routers. Goals: make network robust to failures and attack, maintain spare capacity, reduce operational costs. New challenges: What topology to use? How to find paths? How to identify destinations?

- Hosts assigned topology-dependent addresses
- Routers advertise address blocks("prefixed")
- Routers compute "shortest" paths to prefixes
- Map IP addresses to names with DNS

What is a Protocol?

- Sequence of communications used to conduct some activity in a distributed system
- Protocols are widely used in networks, Figure out how fast to send data, discover paths to destinations, replicate data, endcode data into transmittable patterns, etc.
- Protocols often organized into "suites" or "stacks", Handle collection of activities associated with particular environmental, e.g. TCP/IP(Internet), Infiniband(Data Center), Bluetooth(IoT).

Networks have protocols to

- Routing protocols
- Transport protocols
- Encryption protocols
- Address resolution protocols
- Service discovery protocols

Protocol Stacks
The TCP/IP Protocol Stack: OSI Model, TCP/IP Model. Data Protocols & Control Protocols Each layer of protocol stack encapsulates data passed to it. Each forwarding layer insepcts data only at that encapsulation layer.
Network Addressing
Different Layers Uses Different addresses

- Application layer: URLs, Domain names
- Transport layer: Port numbers
- Networking layer: IP addresses
- Datalink & physical layer: MAC Addresses

Can We Use TCP/IP for IoT? Yes, but IoT introduces additional challenges:

- Very tight power/compute constraints
- Need to work closely with wireless
- Need to address applications, not just interfaces

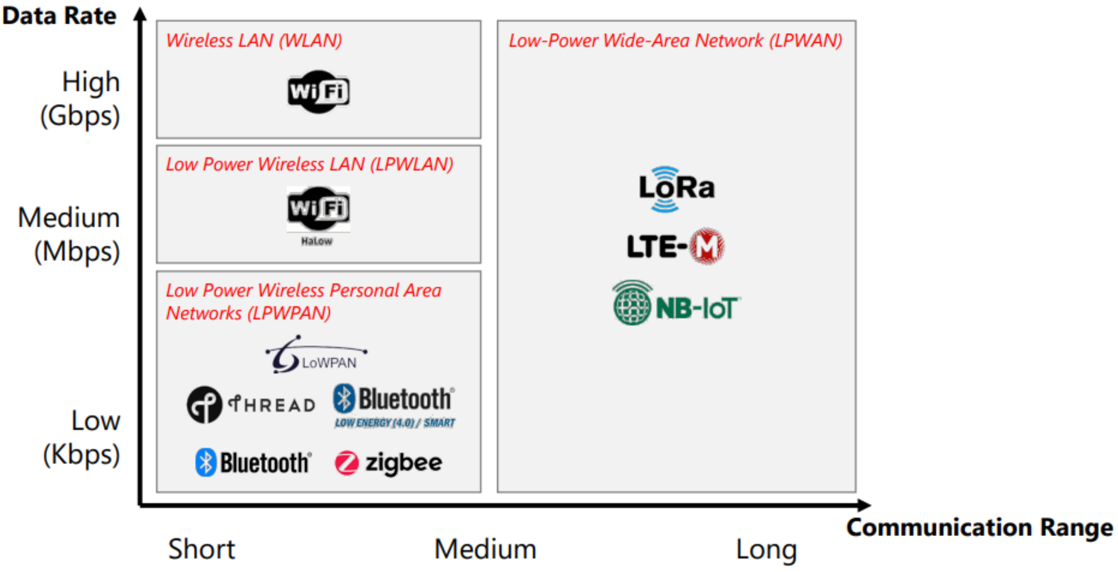


Figure 1: Different IoT Protocols for Different Environments.

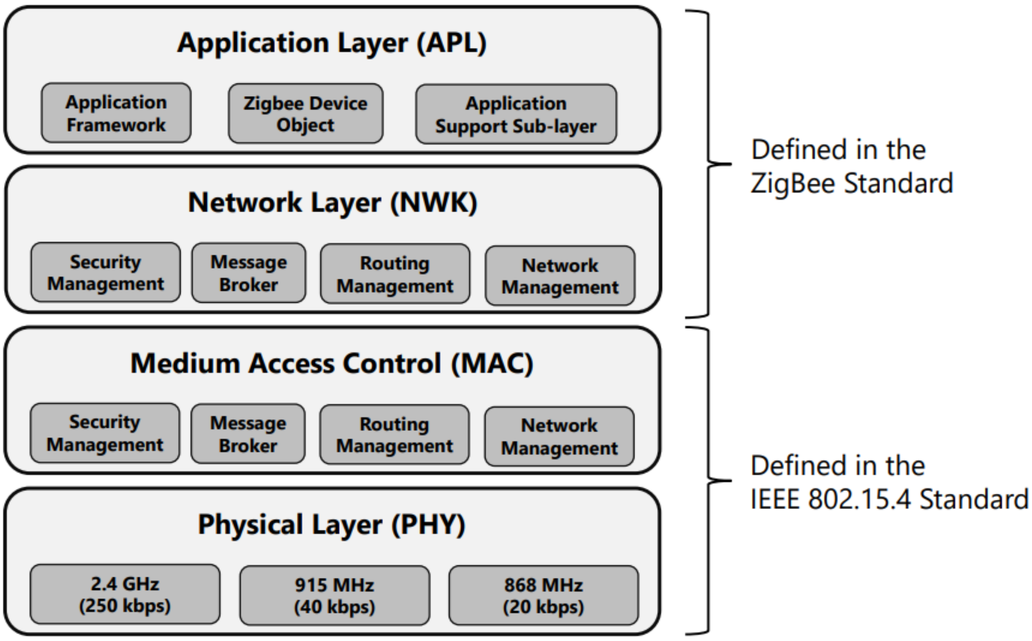


Figure 2: Zigbee Protocol Stack.

Also, creating new protocols can help lock-in and market control. Bad for innovation but good for security.
Common IoT Protocols: **Intra-domain vs. Inter-domain**
Internet routing works on two levels:

- Each AS runs an intra-domain routing protocol internally
  - Establishes routes to internal prefixes and between routers
  - Example protocols: OSPF, IS-IS
  - Run "Interior Gateway Protocol" (IGP) within ISPs
- Each AS runs an inter-domain routing protocol on links to neighboring ASes

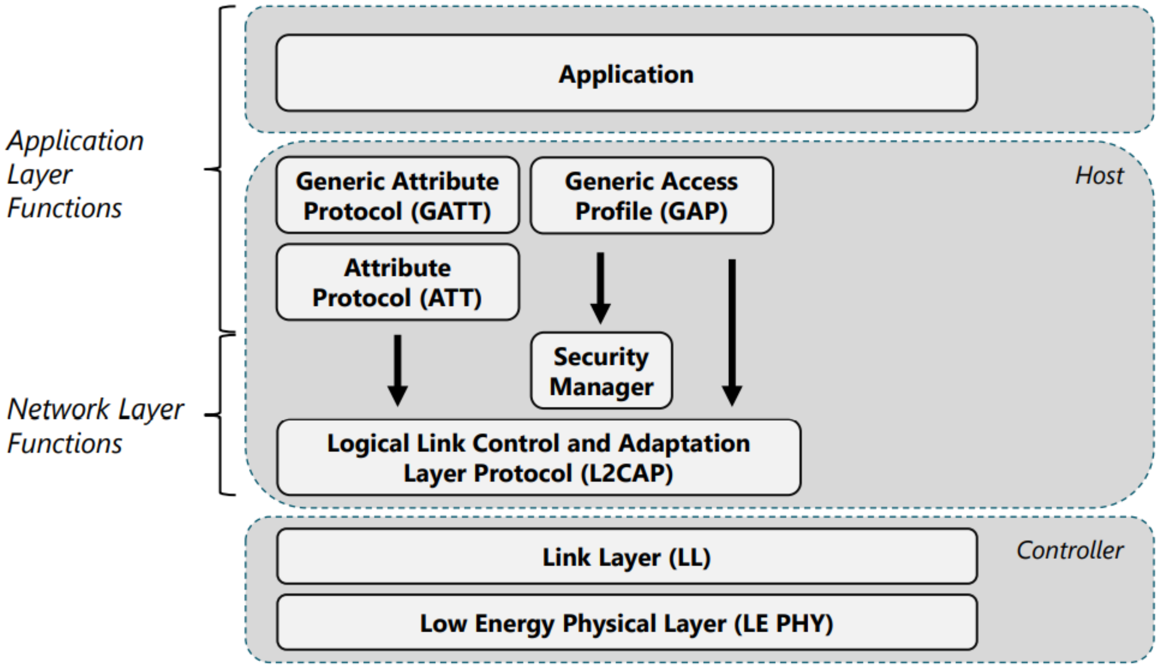
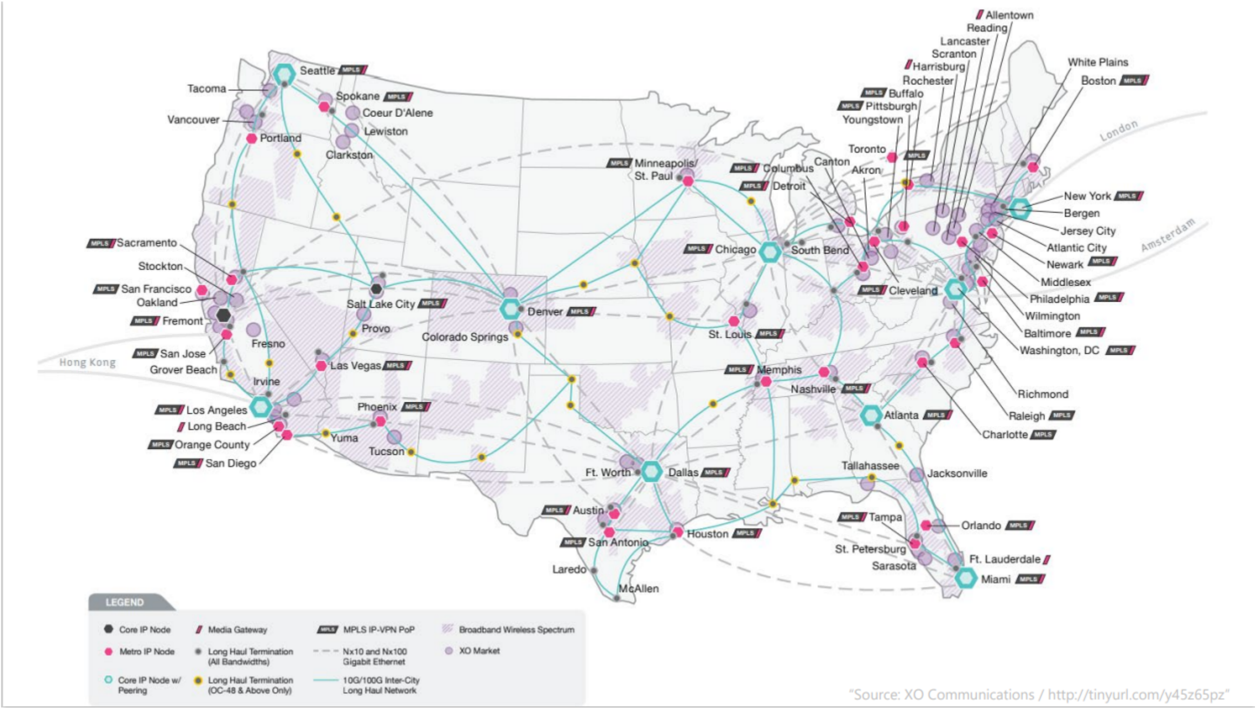

Application Layer Functions
Network Layer Functions
Application
Host
Generic Attribute Protocol (GATT)
Generic Access Profile (GAP)
Attribute Protocol (ATT)
Security Manager
Logical Link Control and Adaptation Layer Protocol (L2CAP)
Controller
Link Layer (LL)
Low Energy Physical Layer (LE PHY)

Figure 3: Bluetooth Low Energy Protocol Stack.

- Establishes routes to external destinations
- Border Gateway Protocol (BGP)
- Use "Border Gateway Protocol" (BGP) to connect ISPs. To reduce costs, peer at exchange points (AMS-IX, MAE-EAST)



"Source: XO Communications / http://tinyurl.com/y45z65pz"

Figure 4: XO Communications Backbone.

Example 1.1 (XO Communications Backbone). The dots are locations where XO Communications provides service to its users. And the lines are links. So what you do as ISP is you look at your market and you figure out where to place routers. The locations where you put routers are known as points of presence. Typically, different ISPs contract with third parties which already own fiber. A lot of these companies that already own fiber are train companies because train companies happen to already own these long secs of land that crisscross the United States. So train companies have gotten into the business of creating optical fiber deployments and they resell to ISPs.

Layer 2 vs Layer 3 forwarding

L3 Routing Proactively Builds State: Control Messages, Routing
L2 Switching Relies on Broadcast

Network Virtualiztion

- Divide up hosts into logical groups called VLANs
  - Like virtual machines, but for LANs (creates "virtual networks")
  - VLANs isolate traffic at layer 2
- Each VLAN corresponds to IP subnet, single broadcast domain
- Ethernet packet headers have VLAN tag
- Bridges forward packet only on subnets on corresponding VLAN

There's a lot of virtualization technologies and networks which are similar to this like VRFs, VXLAN and so on. They all kind of work in the same way, they all kind of take the networks and divide them up into pieces. When you build networks, VLANs are really important to use. Virtual networks are very important because they segment your network up and they can keep your private data away from your public data. So they're very important security primitive.

Delivery Methods

- Unicast
  - One source, one destination
  - Widely used (web, cloud, streaming; many protocols)
- Broadcast
  - One source, all destinations
  - Used to disseminate control information, perform service discovery
- Multicast
  - One source, several (prespecified) destinations
  - Used within some ISP infrastructures for content delivery, overlay networks
- Anycast
  - One source, route to "best" destination
  - Used in DNS, content distribution, service selection

Multicast Approaches

Source-Specific Trees

- Each source is the root of its own tree
- One tree per source
- Tree consitst of shortest paths to each receiver

Shared Tree

- One tree used by all members of a group
- Rooted at "rendezvous point" (RP)
- Less state to maintain, but hard to pick a tree that's "good" for everybody
- Ideally, find a "Steiner tree" minimum-weighted tree connecting only the multicast member(NP-hard)
- Instead, use heuristics(E.g., find a minimum spanning tree)

2 Week 2 Lecture: Devices: IoT circuits

3 Appendix

List of Definitions and Theorems

Todo list