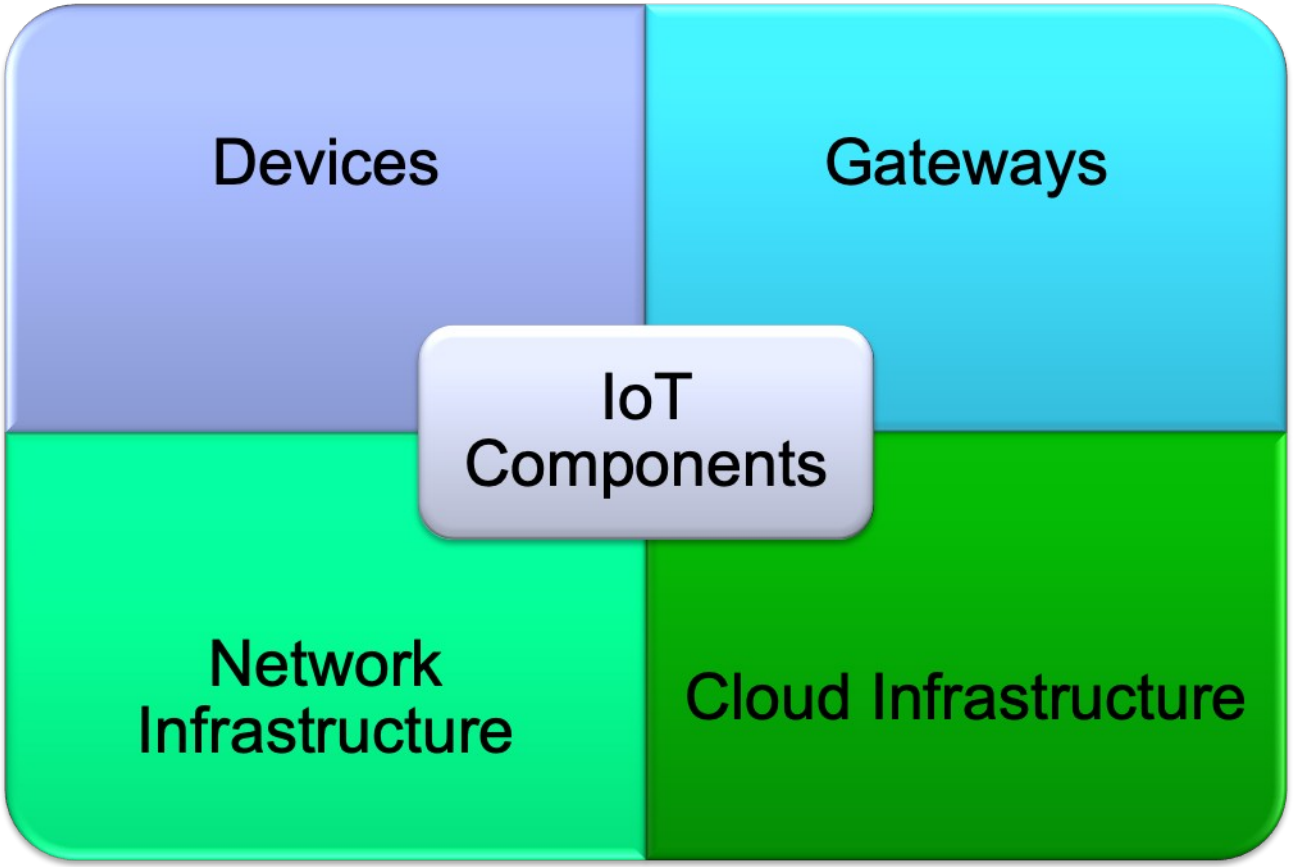
Lecture 10
IoT and Low-power Connected Devices

Fall 2019

Internet of Things (IoT)

- Network of the things and that can communicate
  - Wearables: Smart watches, health monitoring devices
  - Mobile devices: Smart phones, drones
  - Smart home devices and sensors: Surveillance systems, smart appliances, light bulbs, door locks,…
- Main driving forces of IoT:
  - Low-cost wireless devices
  - Big data analysis
  - Machine to machine (M2M) type communications

Internet of Things (IoT)



IoT Requirements

Application	Range	Mo-bility	Device characteristics	Service characteristics	Suitable networks
• Connected car • Fleet management • Remote health monitoring	~1000m	Yes	Rechargeable battery	Managed service, highly secure	• Cellular • Satellite
• Smart metering • Parking meter	~1000m	No	Low rate, low power, low cost	Managed service	• Cellular • Dedicated network
• Hospital asset tracking • Warehouse logistics	~100m	Yes	Low rate, low power, low cost	Enterprise-deployed	• WiFi • RFID
• Industrial automation • Home automation	~10m	No	Low rate, low power, low cost	Subscription-free	• Zwave • Zigbee • Wifi • Powerline
• Personal activity • Local object tracking • Point of sale	~1m	No	Low rate, low power, low cost	Subscription-free	• Bluetooth • NFC

This table is taken from Henning Schulzrinne's presentation: '5G-Separating Hype from Promise'.

Wireless Technologies used by IoT

- **Telecommunication systems:** LTE, GSM, etc.
- **Wireless LAN:** Wi-Fi, Wimax,
- **Low-power, short range:** Bluetooth, Zigbee, Z-wave, RFID, Near-field communication (NFC)
- **Others:** Satellite, broadcast, fixed access networks
- Depends on the requirements (rate, latency, reliability, power, range, etc.)

TCP or UDP?

- High number of devices → high number of flows
- Establishing/terminating each session separately might be costly.
- Usually small packets sent over low-power and lossy networks (LLNs) with long-lasting sessions (called *long association*) → UDP is a better choice.
- Multicasting to many IoT devices → UDP
- If transport is over cellular network, short association with TCP might be a better choice since it can handle the overhead in a more robust network.

Scalability of IoT Network - Addressing

- More than 75 *billion* devices to be connected by 2025 (today around 26 billion devices)
- 2^{32} = 4,294,967,296 unique IPv4 addresses
- IoT growing speed is enormous --> Subnetting is not an effective solution anymore
- Solution: IPv6 with >10^{38} unique IP addresses with support for IPv4

Modifying IP for IoT – 6LoWPAN

- Consider **IEEE 802.15.4**
  - Low-rate wireless personal area networks (LR-WPANs)
  - Simple, flexible and provides low-power/low-data-rate communication
- **6LoWPAN**: IPv6 over low-power wireless personal area network
- **Header Compression**: 40-byte IPv6 and 8-byte UDP headers can be compressed down to as low as 6 bytes.
- **Fragmentation**:
  - IPv6 minimum allowed MTU: 1280 bytes to reduce header overhead
  - 802.15.4 fixed MTU size: 127 bytes since most payloads are a few bytes
  - Requires fragmentation at layer 2

Communication Models and Requirements

- **Device-to-cloud**: IoT device directly connects to an Internet cloud service.
- **Device-to-gateway**: A gateway is an intermediate operator for IoT devices for security, data translation and other operations.
- **Device-to-device**: Two or more devices directly communicate using protocols like Bluetooth, Z-Wave or ZigBee.
- Communication is highly asymmetric: either uplink or downlink is dominant, depending on the application
- Highly distributed and crowded (up to thousands of devices per AP)
- **Example:** In IEEE 802.11ah, **Restricted Access Window** partitions nodes and allows only a set of nodes to transmit each time.

Security in IoT

- Consider **IEEE 802.15.4**
- **Advanced Encryption Standard** (AES) with 128-bit key length
  - Block cipher: operates on fixed-size blocks of data
  - Uses linear operators and non-linear substitution
  - Also validates the data using message integrity code (MIC)
- If enabled, uses up to 14 Bytes from the payload field.
- Security is a huge concern since little authentication control is possible for dynamically changing plug-and-play type of networks.

Energy Limitations

- Mostly low-power and energy-limited devices
- IEEE 802.11ah (Wi-Fi HaLow)
  - IoT devices stay in 'low-power state' and 'wake up' either periodically or at every *target wake time* (TWT)
  - Target wake time (TWT): Access point defines times when an IoT devices 'wakes up' and accesses the network.