Internet of Things 2017/2018

The Things

John Carpenter, 1982

Johan Lukkien

Guiding questions

- What to think about things and how are they connected?

Resource limitations

- *Memory*: available flash (‘program code’) and ram
- *Processor*: Mhz, instruction set expressive power, address width, ability to manage its power
- *Energy*: available Joules and how they are replenished
- *Communication*: required transceive power, bps, complexity of protocols

- These are connected, mainly through energy
  - Ram required power to retain state
  - Processor complexity and Mhz require energy
  - Low memory needs fewer address bits
  - Simpler network protocols and smaller bandwidths lead to lower power transceivers

RFC 7228: devices

- Three classes representing memory (hence processor) limitations

- **C0**: dependent on proxies for secure Internet inclusion
- **C1**: only low resource protocols
- **C2**: can run most Internet protocols
- (**C9**: phone, tablet, desktop)

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

Energy limitation and communication policies

Name	Type of energy limitation	Example Power Source
E0	Event energy-limited	Event-based harvesting
E1	Period energy-limited	Battery that is periodically recharged or replaced
E2	Lifetime energy-limited	Non-replaceable primary battery
E9	No direct quantitative limitations to available energy	Mains-powered

Table 3: Classes of Energy Limitation

Name	Strategy	Ability to communicate
P0	Normally-off	Reattach when required
P1	Low-power	Appears connected, perhaps with high latency
P9	Always-on	Always connected

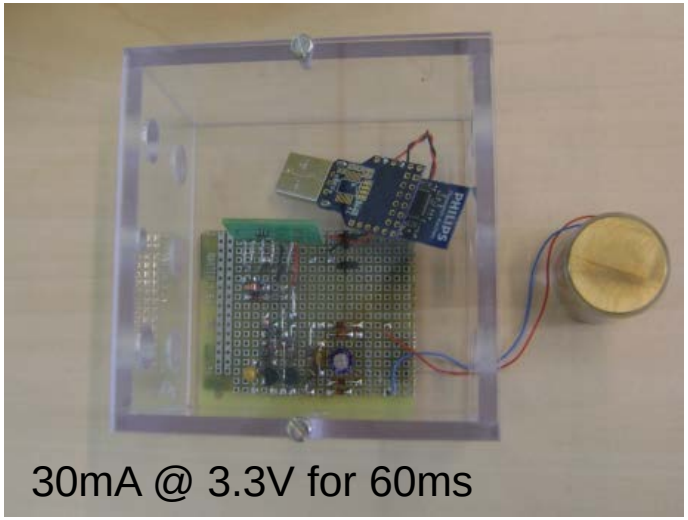
Table 4: Strategies of Using Power for Communication

Some private taxonomy

	Flash	RAM	Address space	Processor (type)	OS	Energy	Operation	Actively reachable	Example
A	small code memory	several bytes	<= 8bits	~100Hz	no	External, or battery + wakeup	Externally activated, simple read/write	not designed for reachability via multi-hop	RFID tag, ISO 18000-6c
B	<= 32K	Few hundreds	<=16 bits	~1Mhz TMS430	no, or simple executive	mechanical	mechanically activated, just generates some data	no; needs proxy	power switch
C	<=32K	Few hundreds	<=16 bits	~1Mhz TMS430	Contiki, TinyOS	battery	simple, fixed external behavior, needs proxy, simple sensing	duty cycled, needs proxy	simple sensor mote
D	<=32K	~10K	<=16 bits	~1Mhz TMS430	Contiki, TinyOS	battery + recharge	capable of managing most constrained IP protocols, sensing, actuating, processing	self-managed on/off behavior	Crossbow
E	<=256K	~32K	<=32 bits	~1-10Mhz ARM	Contiki, TinyOS	battery + recharge, mains	complete IP endpoint behavior, limited storage	yes	Jennic mote
F	~GB	~500Mb	32 bits	~Ghz ARM	Linux	battery + recharge, mains	full fledged embedded computer system	yes	Rasberry PI
G							phones, laptops, servers		

Example: A battery-less light switch

- The switch is pressed.
- The node *turns on* and sends a Route Request broadcast message for a known destination.
  - it boots an OS in the process!
- Using Route Reply, it finds the route to the luminaries.
- Using the discovered route, the node transmits the control signal (turn on/off) to the luminaries.
- The luminary node acknowledges the reception of the control signal.
- The switch node does multiple retries to transmit that control signal as long as the node stays on and until an ACK is received.



Running FreeRTOS and capable of transmitting compressed IP packets (6LoWPAN).

From: *6LoWPAN: IPv6 for Battery-less Building Networks,* MSc thesis of N.A. Abbasi, TU/e

Functionality of things

- ‘Things’ must be capable to perform the required sensing, actuation, computation, communication
  - functional requirements

- In addition, because they are many:
  - (secure) bootstrap, (secure) network association
    - upon (re)starting a device must load its code from a trusted source
    - it must join the correct network
  - secure communication
  - (secure) software update, *over the network*
    - updates are inevitable and must remain safe
  - … part of the *life cycle*

Concerns and management

- can it join a network?
  - secure bootstrapping
- can it be configured?
  - adapting operational parameters
    - e.g. sensing, communication frequency
- can it be updated (over the air)?
  - new firmware, new software, new application components
- can it run IP?
  - serve as IP endpoint
- can it secure itself?
  - independent node

- A,B,C: need trusted partner (proxy)
- A,B: very little; C: limited
- From D onwards
- From E onwards; D runs limited protocols
- A,B,C: need trusted partner; D: limited

Some private taxonomy

	Flash	RAM	Address space	Processor (type)	OS	Energy	Operation	Actively reachable	Example
A	small code memory	several bytes	<= 8bits	~100Hz	no	External, or battery + wakeup	Externally activated, simple read/write	not designed for reachability via multi-hop	RFID tag, ISO 18000-6c
B	<= 32K	Few hundreds	<=16 bits	~1Mhz TMS430	no, or simple executive	mechanical	mechanically activated, just generates some data	no; needs proxy	power switch
C	<=32K	Few hundreds	<=16 bits	~1Mhz TMS430	Contiki, TinyOS	battery	simple, fixed external behavior, needs proxy, simple sensing	duty cycled, needs proxy	simple sensor mote
D	<=32K	~10K	<=16 bits	~1Mhz TMS430	Contiki, TinyOS	battery + recharge	capable of managing most constrained IP protocols, sensing, actuating, processing	self-managed on/off behavior	Crossbow
E	<=256K	~32K	<=32 bits	~1-10Mhz ARM	Contiki, TinyOS	battery + recharge, mains	complete IP endpoint behavior, limited storage	yes	Jennic mote
F	~GB	~500Mb	32 bits	~Ghz ARM	Linux	battery + recharge, mains	full fledged embedded computer system	yes	Rasberry PI
G							phones, laptops, servers		

What's new with IoT?

- There are **many** things
  - #things / person >> 1 (50B in 2020)
  - hence, things need to talk to *each other* or to a *database*
    - about …..?
  - self-* properties, autonomy
    - self management, self healing, …
  - scalability, at access networks
    - many things sharing your wireless LAN
    - special infra structure outdoor
- Things have **limitations**
  - low processing power, memory, low capacity network
    - size IP packet comparable to available memory
  - sometimes battery operated
  - embedded: no UI
- Their numbers and far-reaching locations enable **entirely new applications**
  - large-scale data collection
  - data-based applications
  - manufacturers probing into the deployed systems
- Their scale and locations comes with **complex concerns**
  - device/data handling, ownership
  - security, safety, application reliability
    - at a compelling scale
  - application development, deployment, management

Guiding questions

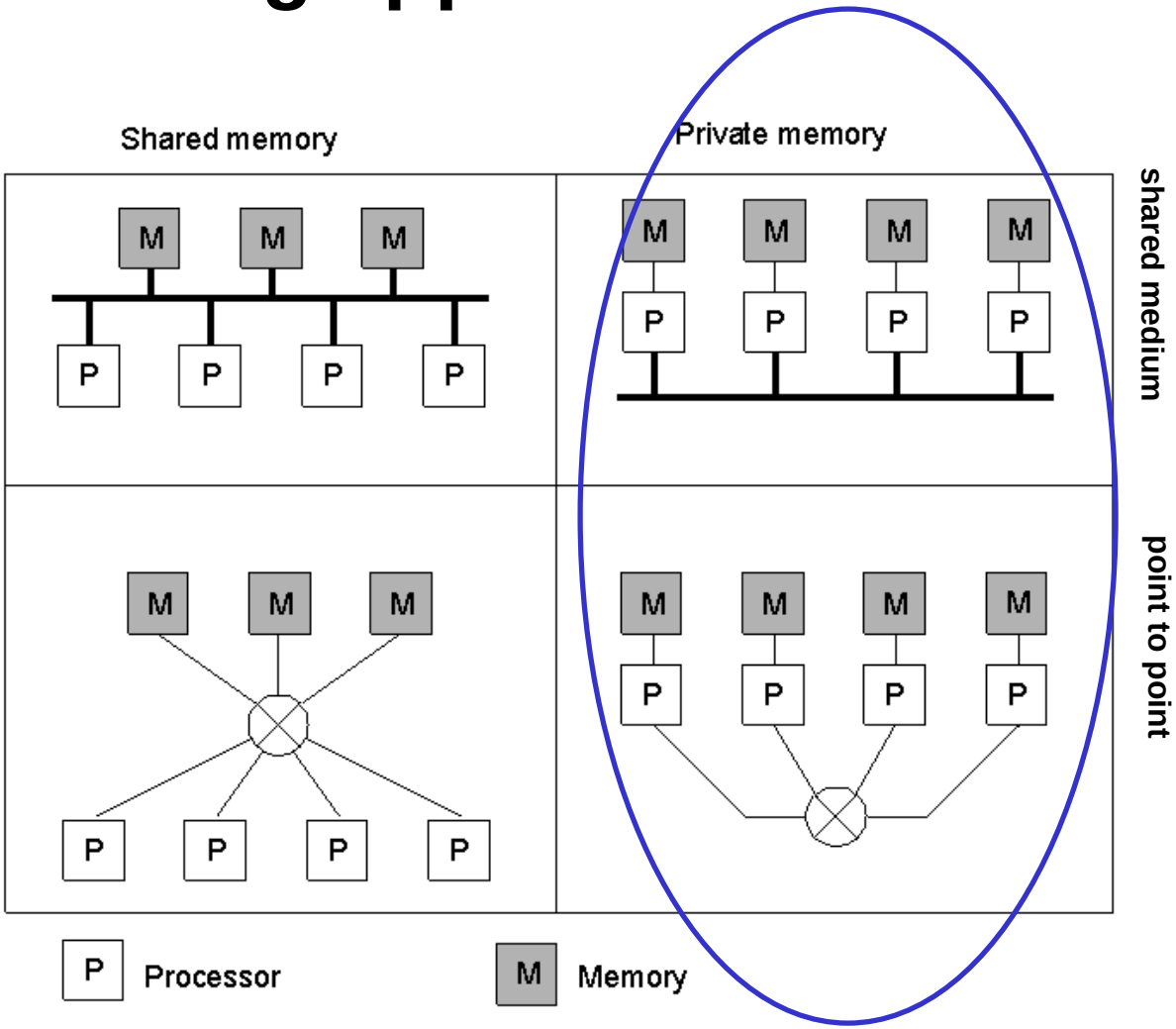
- What to think about things and how are they connected?

How do end points communicate?

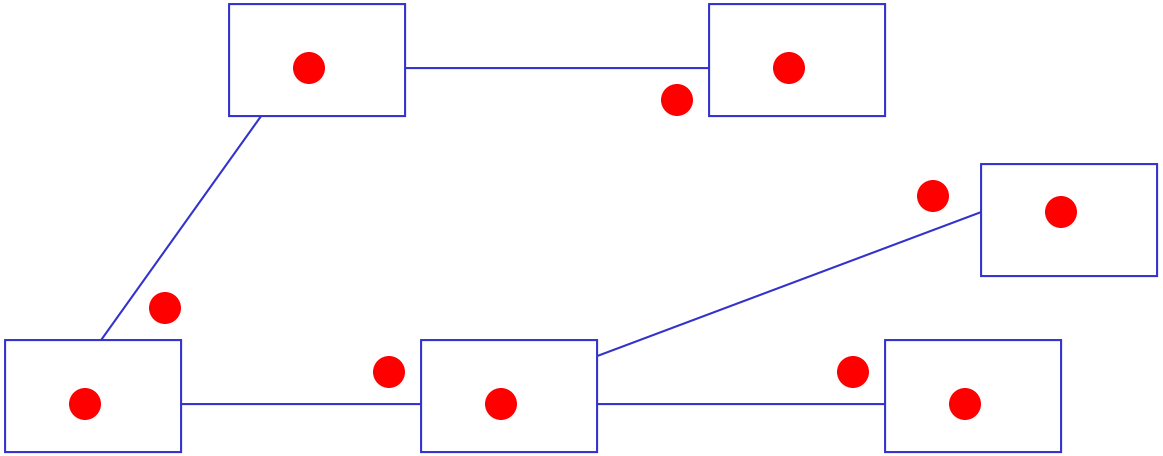
Networking approaches

- Physical neighbors:
  - Shared medium
  - Point-to-point
- In case of physical separation
  - switching
  - connecting networks
  - ... multiple interfaces for some nodes

- Packet oriented
- Full connectivity by
  - (intelligent) flooding
  - routing



Flooding



	Wired	Wireless
Battery	Energy limitations will determine uptime communication behavior and protocols. In principle, the wire could be used for power; and at least for waking up nodes	Energy limitations will determine uptime, communication behavior and protocols; nodes must manage their sleeping behavior; nodes can be mobile
Mains	No real need for low resources except cost and energy; this class captures ‘regular’ office/home infra structure devices	Wireless is there for convenience (absence of other infra - outdoors) and for connecting to mobile wireless nodes; powerful wireless protocols can be used, always on

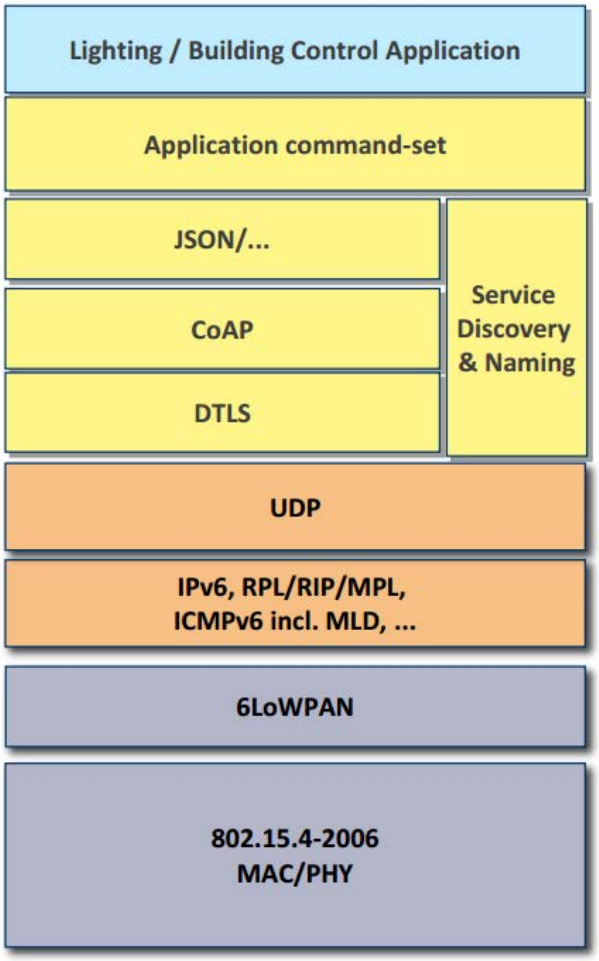
The LANs

Name	Description	Note
IEEE 802.1	Higher Layer LAN Protocols	active
IEEE 802.2	LLC	disbanded
IEEE 802.3	Ethernet	active
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	disbanded
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	active
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	active
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	
IEEE 802.15.7	Visible light communications	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.16.2	Coexistence wireless access	
IEEE 802.17	Resilient packet ring	hibernating
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	hibernating
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	Not yet ratified

- Taken from Wikipedia (Nov. 2015)
- Important wireless:
  - the 3 group (ethernet, PoE)
  - the 11 group ('WiFi')
  - the 15 group (wireless PAN)
- Within IEEE 802.15
  - 1x: Bluetooth
  - 4x: PHY/MAC layer for ZigBee, 6LoWPAN, Thread, WirelessHART, MiWi ContikiMAC, 6Tisch…
- Within the IEEE 802.11 LANs:
  - 11p: ITS
  - 11e: QoS
  - 11s: meshing
  - 11ah: low power, low interference

Example: which (IP) protocols occur in a lighting network?

- Connectivity:
  - 6LoWPAN (= adaptation for IP/802.15.4), UDP, TCP [sometimes]
  - RPL, RIP, MPL: routing, multicasting
  - DTLS: packet based security
- Application
  - Trickle: application protocol for dissemination to all devices in a network
  - RESTful style
    - REST plus HTTP methods
    - CoAP – constrained application protocol
  - DNS-SD using mDNS, or CoAP directory: for service discovery
  - M2M protocols, e.g. MQTT/TCP



Courtesy of Dee Denteneer

Characteristics of wireless communication

- A wireless network is like a shared channel to put data on
  - standards must address this sharing, avoiding destructive interference
- Wireless communication is intrinsically subject to errors
  - received signal is the energy collected over time
  - can always be disturbed by an external party (a different protocol family in same frequency), or by another neighbor than the sender
  - quality depends on environment properties (e.g. reflections)
- Wireless communication is energy-hungry, particularly when compared to the energy used by embedded processors
- Standards must address the unreliability, sharing and energy use

What techniques are applied?

- FDMA: multiple channels
  (frequency division multiple access)
  - channel hopping with synchronization
    - e.g. 802.15.1 (Bluetooth), 6tisch,
  - cell formation / independent domains
    - e.g. 3/4G, IEEE 802.11 (WiFi)
- TDMA: division in timeslots
  (time division multiple access)
  - timeslots with schedules, time synchronization
    - e.g. WirelessHART, DECT, IEEE 802.15.4 in superframe mode
  - in combination with cell formation
- Master-Slave
  - e.g. an access point as master
  - beacon-based signaling
    - e.g. IEEE 802.11 (WiFi), Bluetooth, IEEE 802.15.4
- CSMA: 'try before you cry'
  (carrier sense multiple access)
  - Clear Channel Assessment: Aloha
  - with collision avoidance, detection or resolution
    - e.g. IEEE 802.15.4 (ZigBee): random distribution of retries
  - with priority
    - e.g. IEEE 802.11e (WiFi + QoS)
- CDMA
  (code division multiple access, as in 4G)
  - concurrent access of the medium with coded packets
  - admits decoding even with interference
- Regulation
  - duty cycle restrictions (e.g. 1% per station)
  - frequency assignment

	Wired	Wireless
Shared medium	CSMA/CD: coax ethernet CSMA/CR: CAN TDMA token passing: profibus Master/Slave: ethercat (,profibus)	MA/CA: (pure) Aloha CSMA/CA: Wifi, Zigbee TDMA: Wireless Hart Master/Beaconing: Wifi, Zigbee FDMA + channel hopping: bluetooth (low energy), 6tisch CDMA: virtual point to point (4G), Chirp Spread Spectrum UWB
Point to point	Switched ethernet: PoE Common way to set up larger networks using switches and routers	FDMA Dedicated frequencies for long-haul transport: satellite

	Wired	Wireless
Outdoor	No common infra structure available; some initiatives via light poles or other relatively dense infra	City WiFi 4G/5G: LTE adaptation, LongRange low power WAN technologies
Indoor	Standard wired infra structure using UTP, fiber, switches, bridges and routers	WiFi Bluetooth IEEE 802.15.4 based technologies

Energy, in low capacity environment

- Radio communication is a major contributor to energy consumption
  - don't use it ☺

- Applied techniques (combinations, need support at multiple layers)
  - asymmetry
    - low-power nodes are 1 hop away from well-powered infra
  - control the transmit / receive power
    - trade connectivity for energy
  - duty cycle
    - switch node or radio on and off periodically
  - demand driven
    - event driven control of radio (wakeup radio, or push mode) with asymmetry
  - push / pull strategies
    - let the low power partner always be the first
  - trade power for range and throughput
    - special network technologies, special physical layers

Metrics (which is how to judge all this)

- throughput
  - number of bytes per time unit
  - for a station: bytes per interval
- latency or delay
  - time difference in initiation of a transmission and the start of the receipt
  - consist of processing delay, transmission delay and queueing delay
- jitter
  - variations in timing, e.g. delay jitter, throughput jitter
- fairness, ability to prioritize
  - fairness: bound on delay in access to a transmission channel
  - or fair share in competition
- overhead
- scalability
  - as utilization
    - increasing the amount of communication
    - increasing # stations
    - e.g. CSMA/CA scales badly when increasing # stations while TDMA scales well
  - as dimensioning
    - LoRaWan can scale the number of gateways with the number of low-power nodes
- predictability
- reliability
  - e.g. resilience agains interference
- power
- range

Qualitative metrics

	Range	Power	Resilience against Interference	Predictability	Scalability (utilization)	Overhead	Prioritization	Fairness	Jitter	Latency	Throughput
FDMA	o	o	+	o	o	-	o	o	o	o	+
TDMA	o	o	o	+	+	-	o/+	+	+	-	o
CSMA/CA (+QoS)	o	o	o	-	-	+	o(+)	+	-	+	o
CDMA, spread spectrum	+	+	+	o	+	o	o	o	o	o	o
Master / Slave	o	o	o/+	+	+	-	+	o	o	+	-
Cell formation / domains	o	o	+	o	+	-	o	o	-	-	+
Asymmetry	o	+	o	o	o	o	o	o	o	+	o
Duty Cycling	o	+	o	o	+	+	o	+	-	-	-

- +: improves (e.g. ‘Latency +’ means improves (reduces) Latency)
- -: makes worse
- o: no effect/not applicable

Guiding questions

- What to think about things and how are they connected?