SCC.306 Internet Applications Engineering
Embedded Computing and the Internet

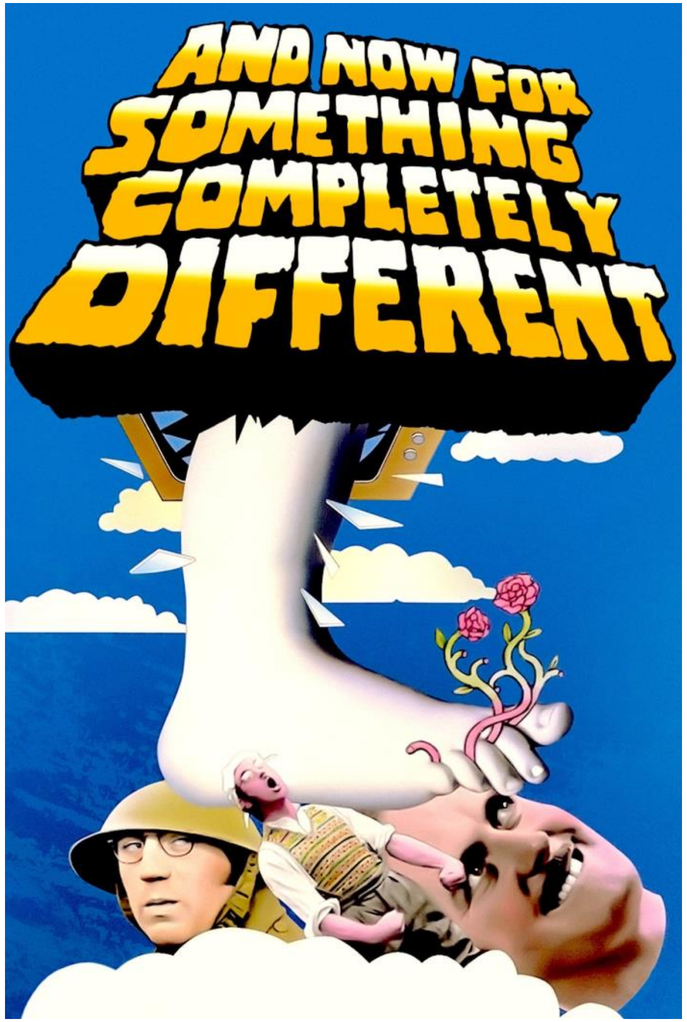
24th October 2024

Matthew Bradbury

Agenda

1. Avoid limiting assumptions of what an internet connected device is
2. The different approaches and considerations of
    1. Internet of Things
    2. Vehicles

Remember: internet applications are not just the web!



Avoid limiting assumptions

- Not all computing systems are connected to the internet
  - Some have no connectivity
  - Some work on private ad-hoc networks
  - Some may interact in limited ways with online systems
- Networking structure is changing to meet the demands of these devices
- Not all systems will be running common software
  - Custom embedded OS / code on bare metal

Mavic 2 ©DJI

nRF52840 Dongle ©Nordic Semiconductor

Westfield POD

Embedded Systems Characteristics

- Low resources
  - Limited CPU power
  - Limited memory (both RAM and stable storage)
  - Low communication data rates
  - (potentially) limited battery power
- Lots of them
  - Need the ability to address these devices

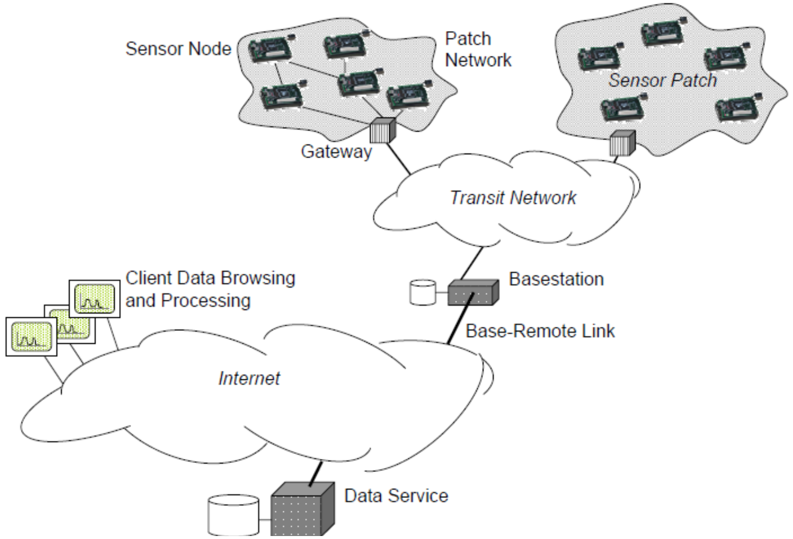
nRF52840 Dongle ©Nordic Semiconductor

Embedded Systems do not exist in isolation

- Embedded systems can exist in isolation
- In general, to provide an interesting service they need to be networked
    - WPAN (wireless personal area network)
    - BAN (body area network)
    - UAV Communication
    - Intranet / Internet

Wireless Sensor Network

- Building health
- Environment monitoring
- Animal / habitat monitoring
- Emergency scenario detection
- Monitor state of industrial equipment – build digital twins



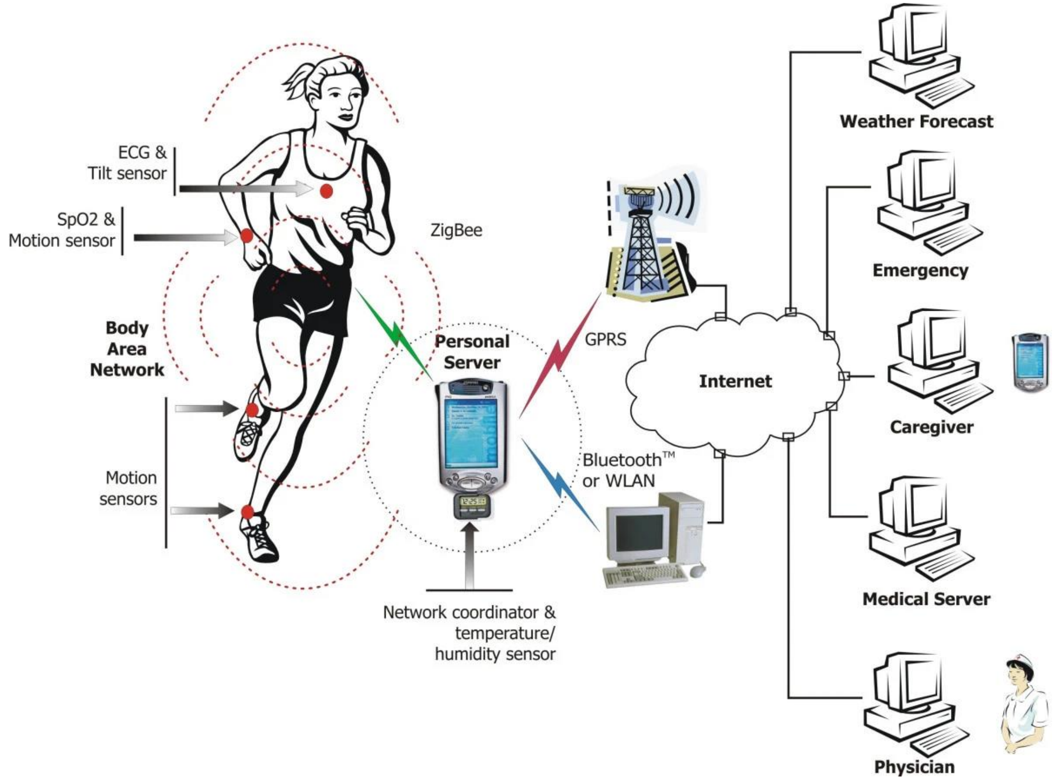
(a) Sealed block

(b) Cylinder with vents and drainage

Szewczyk, R., Polastre, J., Mainwaring, A. and Culler, D. 2004. Lessons from a Sensor Network Expedition. *Wireless Sensor Networks*. , ed.H. Karl, A. Wolisz, and A. Willig. Springer Berlin Heidelberg. 307–322.

Wireless Body Area Network

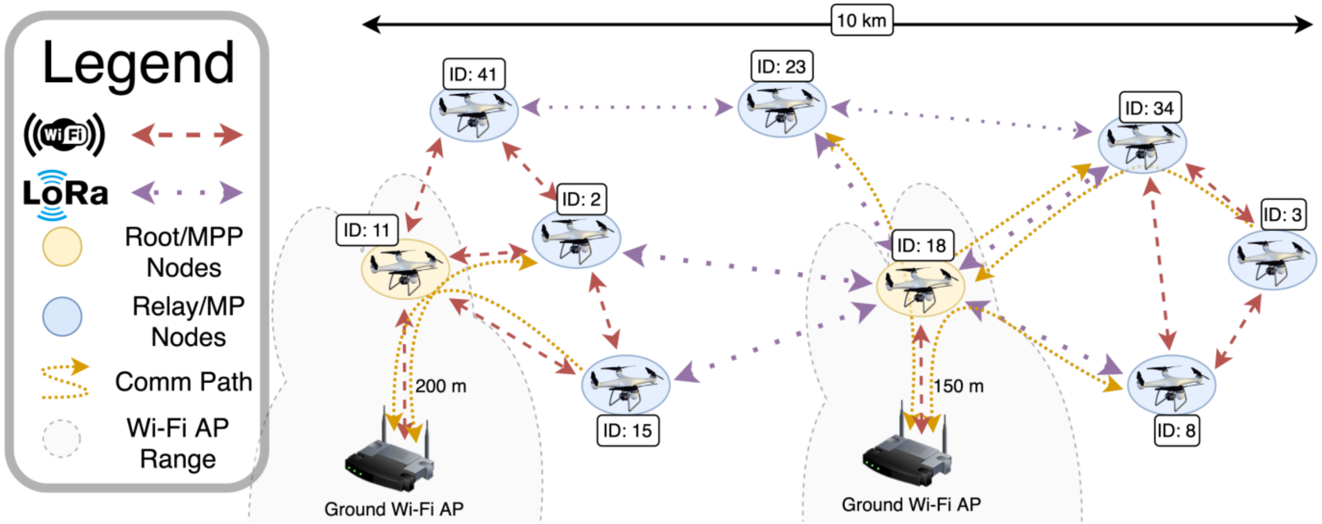
- Monitor a person
- Health indicators
- External and internal sensors
- Send information to local or remote servers



Jovanov, E., Milenkovic, A., Otto, C. *et al.* A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *J NeuroEngineering Rehabil* **2,** 6 (2005). https://doi.org/10.1186/1743-0003-2-6

Unmanned Autonomous Vehicle Networks

- Mobile environment monitoring
- Agricultural and military use cases
- Drones communicating with each other in swarm to autonomously plan actions
- Data mules – physically transfer data without wireless communication



Davoli, L.; Pagliari, E.; Ferrari, G. Hybrid LoRa-IEEE 802.11s Opportunistic Mesh Networking for Flexible UAV Swarming. *Drones* **2021**, *5*, 26. https://doi.org/10.3390/drones5020026

What does this mean for internet access?

- There is a conflict between the resources available and the requirement of existing internet technologies
- Often a focus on performance and utility
- Less of a focus on the resource requirements
- IPv6 is essential – Need to have addresses for a large number of devices

Lancaster University

Differences

Operating Systems

Not all cyber physical systems will be running a common OS

- Drones – PX4 Autopilot (https://www.dronecode.org)
- Embedded IoT – Zephyr (https://zephyrproject.org) / RIOT (https://riot-os.org)
- Automotive
  - Highly complex, large variety of different components
  - QNX RTOS (https://blackberry.qnx.com/en)
  - FPGAs (no OS!)
  - Linux-based electronic control units (ECUs)
- Just a small selection of domain-specific approaches

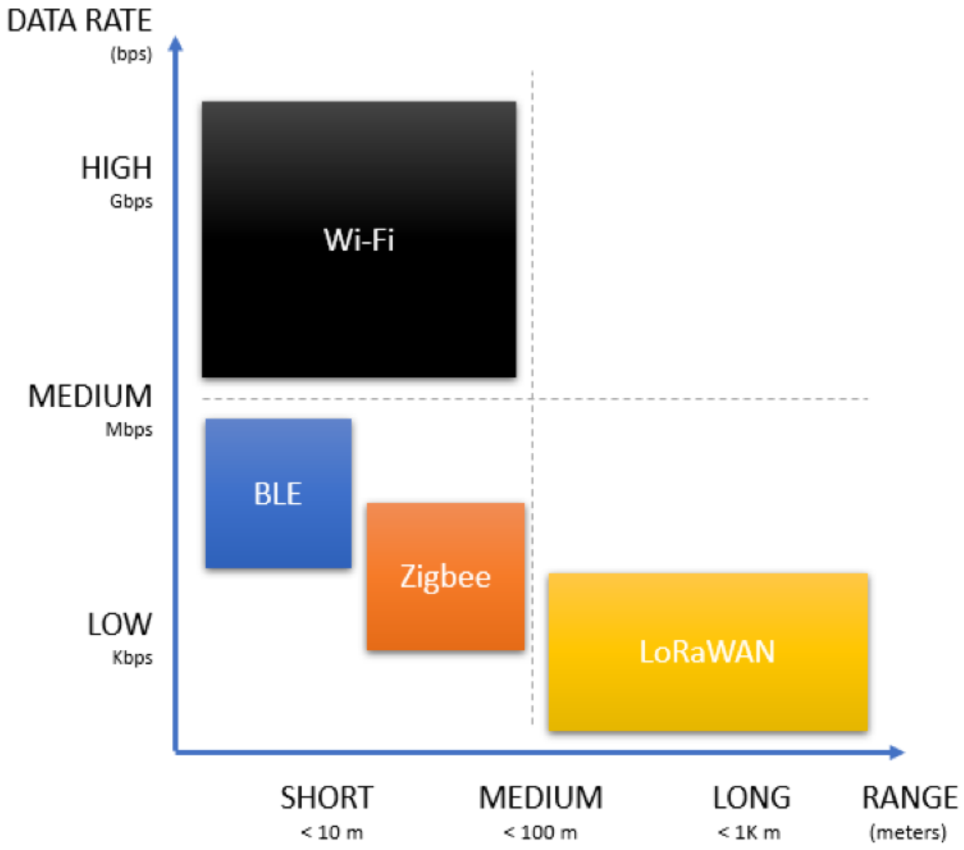
Device Capabilities

- Embedded systems have low computational and memory resources
- Potentially limited battery power (or none)
- Potentially no writable stable storage
- Hardware acceleration for cryptographic operations

Name	CPU	RAM	Flash (ROM)
nRF52840 (IoT)	64 MHz Arm Cortex-M4	256 KiB	1 MiB
Pixhawk 4 STM32F765 (Drone)	216 MHZ Arm Cortex-M7	512 KiB	2 MiB
Cohda MK5 OBU (Vehicle)	1 – 1.2 GHz Arm Cortex-A9	1 GiB	Multiple GiBs Writable

Communication Capabilities

- Typically internet protocols aren’t always used in these systems
- Why?
- Different design decisions needed for:
  - RAM/ROM space optimisations
  - Energy consumption
  - Communication capabilities (low bandwidth, high range)



© Wireless Broadband Alliance https://wballiance.com/guest-blog-wi-fi-lorawan-and-iot-convergence/

Comparing Communication Protocols

- Large variety of approaches with different trade-offs
- How long will it take to deliver a payload?
- What payloads are suitable?
- What is the energy cost?
- What is the communication range?

Name	Transfer Rate	Distance
IEEE 802.15.4 / Zigbee / 6LoWPAN / Thread	250 kbps	~10m
LoRaWAN	27-59 kbps	2-15km
IEEE 802.11p /WAVE / ITS-G5 (vehicular)	3-27 Mbps	Up to 100m
IEEE 802.11ac IEEE 802.11ad IEEE 802.11ah	450 – 1300 Mbps 6.7 Gbps 347 Mbps	Up to 35m 3m Up to 1km

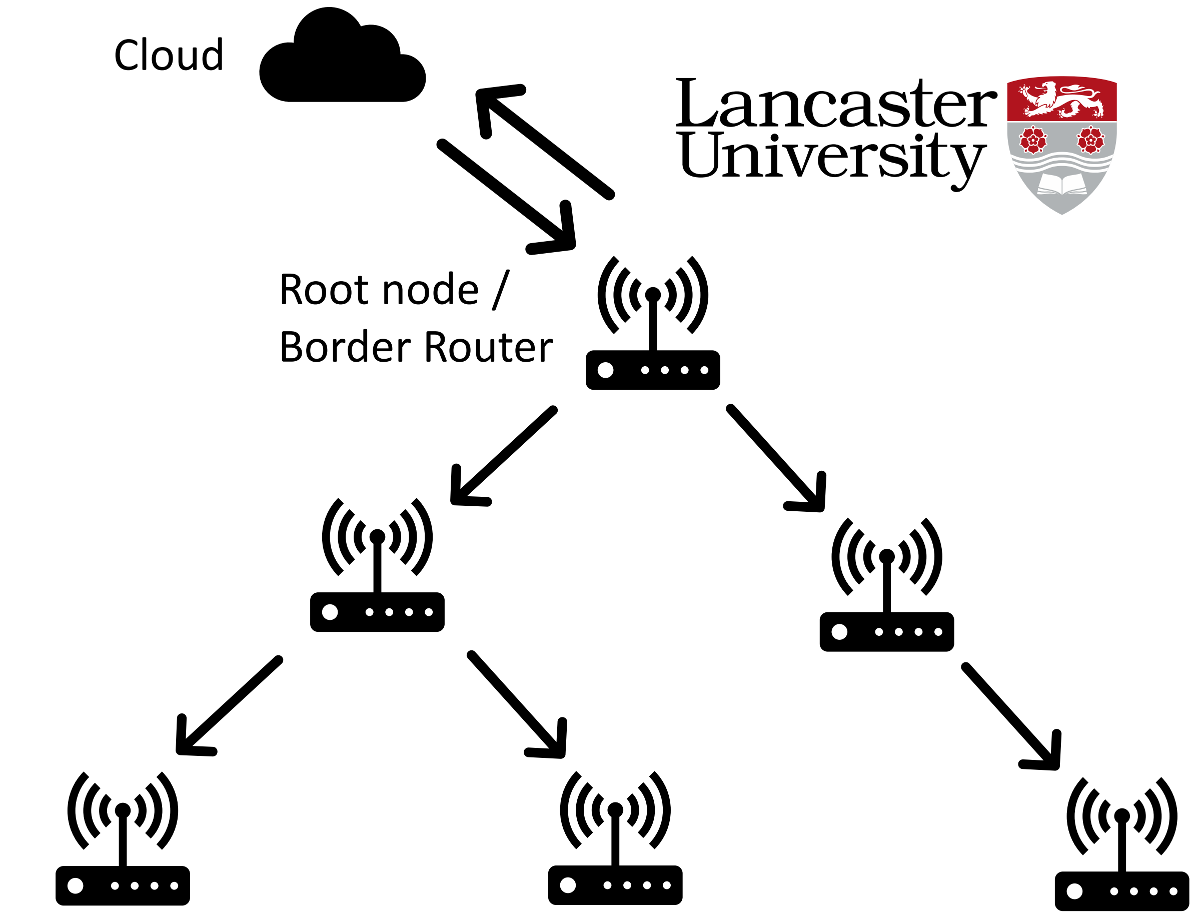
Communication Protocols

Simplified OSI Model	Typical Network	Example IoT stack	Vehicular Network
Security	TLS	DTLS, OSCORE	Complicated
Application	HTTP, SQL, NFS/SMB, RPC, NTP	CoAP, MQTT-SN, NTP, LWM2M	CANopen / CAN FD
Transport	TCP/UDP	UDP	ISO 15765-2 (aka ISO-TP)
Network	IPv4/IPv6	6LoWPAN (IPv6) and RPL	
Link	Ethernet / IEEE 802.11 / Cellular	IEEE 802.15.4 TSCH / BLE	CAN bus MAC and Link Control
Physical	UTP cables / Fibre	Wireless medium	CAN bus physical cable / Ethernet?

Internet of Things (IoT)

6LoWPAN and RPL

- How are IoT devices addressed? – 6LoWPAN
- How are messages routed across an ad-hoc network of IoT devices? - RPL
- Overlay logical directed acyclic graph on network topology
- Threats:
  - Is the traffic encrypted?
  - Manipulate formation of tree



Cloud

Root node / Border Router

DAO: Update parent of node

DIS: Information request

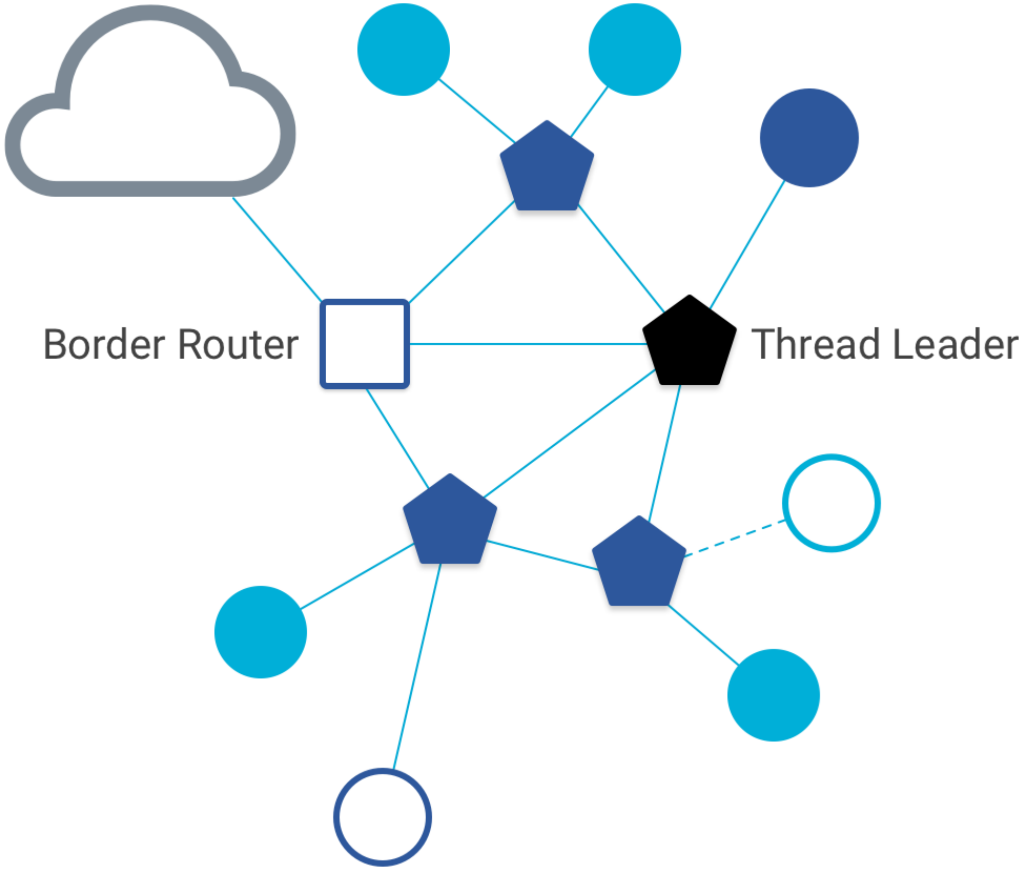
DIO: Information response

https://datatracker.ietf.org/doc/html/rfc6550

Thread

- Another mesh network
- High level of industrial support
- Focus on simplicity and security
- Custom protocol for node discovery and routing (different to RPL)

High diversity in different approaches to mesh networking



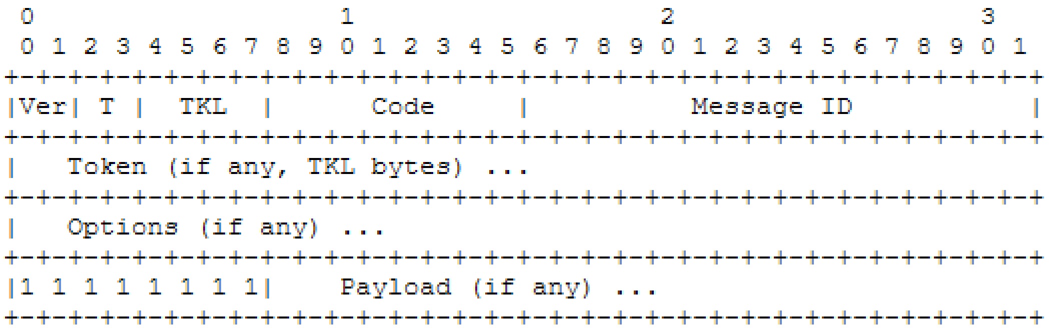
https://www.threadgroup.org

Preference for UDP

- TCP - Reliable and ordered transmission of data
- UDP – No guarantee of delivery or order of delivery
- UDP is much cheaper to implement in terms of both RAM and ROM
  - No need to maintain connection state
  - No need for large buffers to store data that has been received early

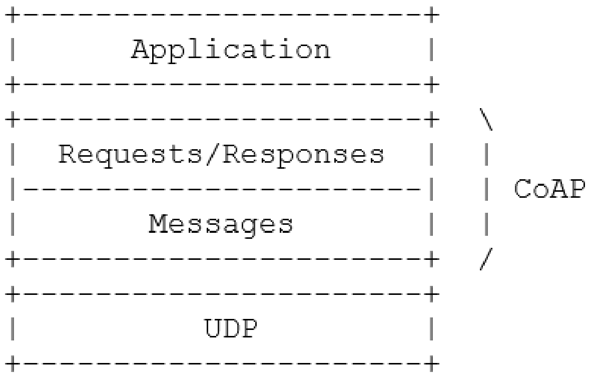
Constrained Application Protocol (CoAP)

- HTTP used to transfer information over the web
- CoAP preferred in IoT deployments
- Used in client-server contexts
- Clients can act as servers



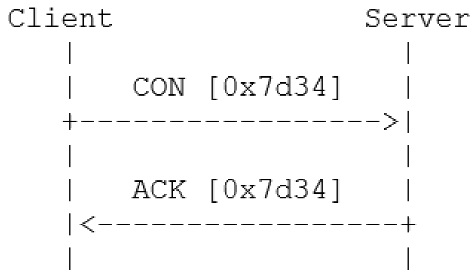
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Ver| T |  TKL  |      Code     |          Message ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Token (if any, TKL bytes) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 1 1 1 1 1 1|    Payload (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: Message Format



```
+----------------------+
|      Application     |
+----------------------+
+----------------------+  \
|  Requests/Responses  |  |
|----------------------|  | CoAP
|       Messages       |  |
+----------------------+  /
+----------------------+
|          UDP         |
+----------------------+
```

Figure 1: Abstract Layering of CoAP



```
Client              Server
   |                  |
   |   CON [0x7d34]   |
   +----------------->|
   |                  |
   |   ACK [0x7d34]   |
   |<-----------------+
   |                  |
```

Figure 2: Reliable Message Transmission

https://datatracker.ietf.org/doc/html/rfc7252

CoAP vs HTTP

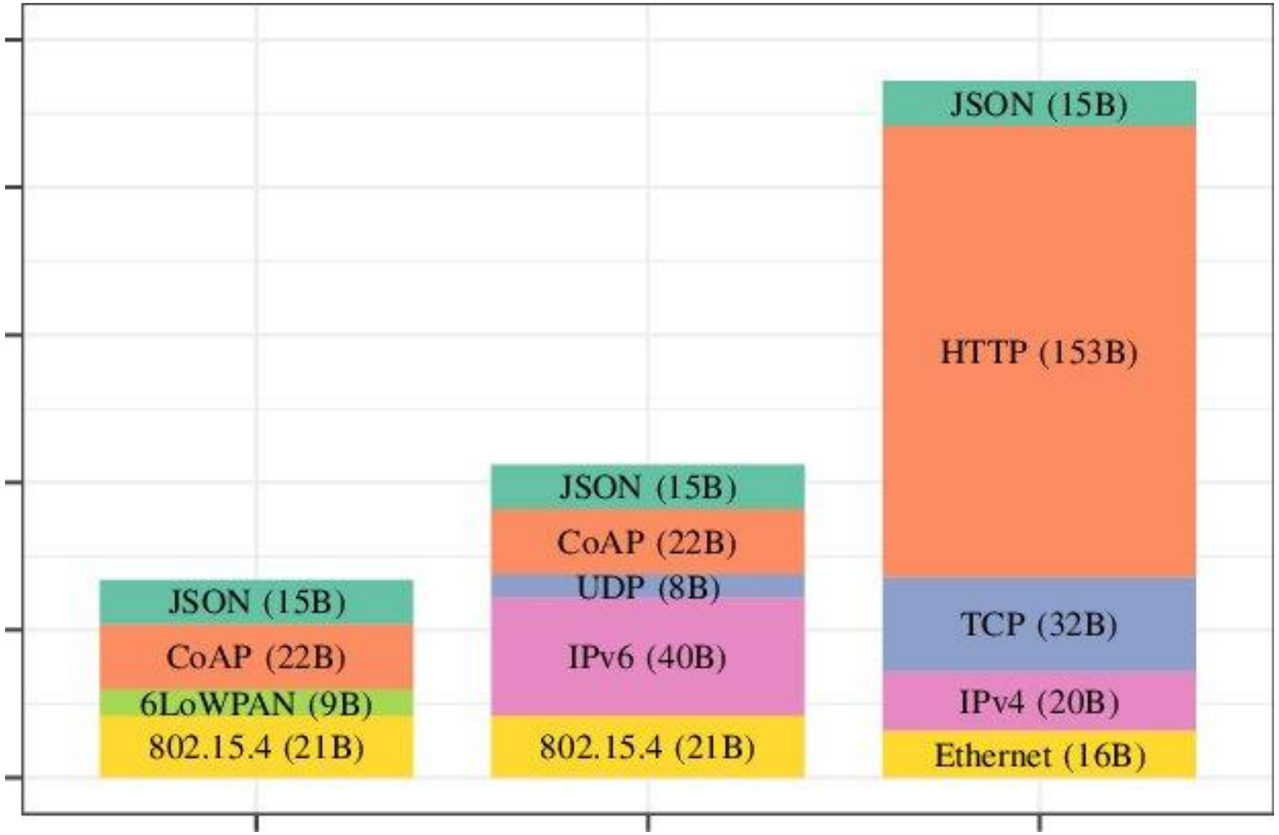
Lancaster University

Description	HTTP	CoAP
Get data	GET	0.01 GET
Submit data	POST	0.02 POST
Replace target with data	PUT	0.03 PUT
Delete a resource	DELETE	0.04 DELETE
Get data and include a body with submission	GET+POST	0.05 FETCH
Partially modify a resource	PATCH	0.06 PATCH
		0.07 iPATCH
Establish a tunnel to a resource	CONNECT	
Describe communication options for a resource	OPTIONS	
GET without a body (only return headers)	HEAD	

https://www.iana.org/assignments/core-parameters/core-parameters.xhtml#codes
https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods

CoAP is much cheaper

- Different optimisation aims for CoAP
- Smaller message sizes
- Smaller implementation
- Less capable than HTTP



S. Meiling, D. Purnomo, J. Shiraishi, M. Fischer and T. C. Schmidt, "MONICA in Hamburg: Towards Large-Scale IoT Deployments in a Smart City," *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 224-9, doi: 10.1109/EuCNC.2018.8443213.

CoAP Demo

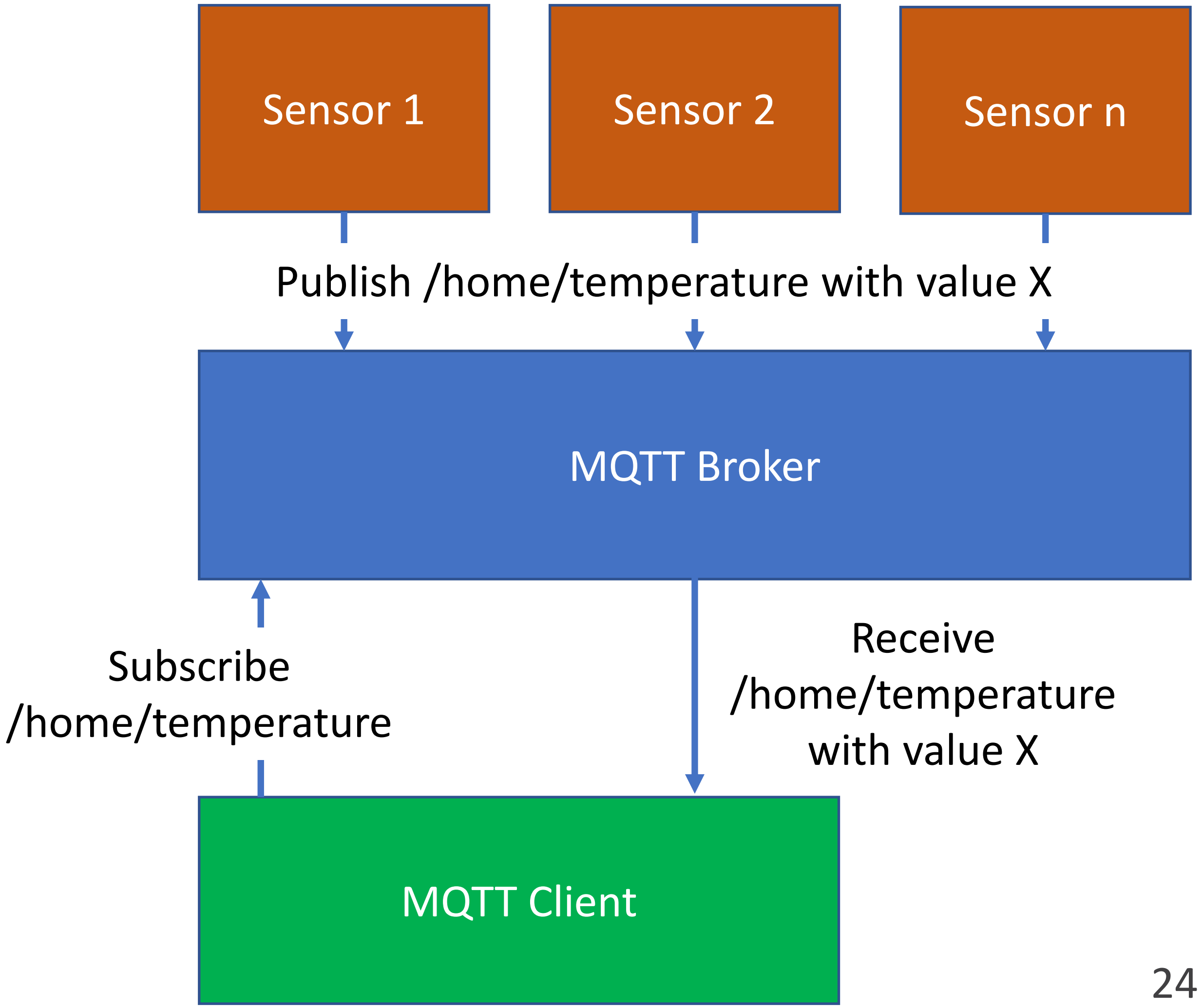
https://github.com/chrysn/aiocoap

```
$ ./server.py

$ ./aiocoap-client -m GET coap://localhost/.well-known/core
$ ./aiocoap-client -m GET coap://localhost/whoami
$ ./aiocoap-client -m PUT coap://localhost/other/block --payload
"Important data"
$ ./aiocoap-client -m GET coap://localhost/other/block
```

MQTT

- A publish/subscribe protocol
- Devices subscribe to a specific topic with a broker
- Other devices publish information about that topic to the broker
- The broker forwards this information on to subscribed devices



Sensor 1
Sensor 2
Sensor n
Publish /home/temperature with value X
MQTT Broker
Subscribe /home/temperature
Receive /home/temperature with value X
MQTT Client

https://mqtt.org/mqtt-specification/

MQTT and MQTT-SN

- MQTT is based on TCP
- TCP is very heavyweight for some implementations
- MQTT-SN is based on UDP and targets highly resource constrained devices
- MQTT-SN is still a pub/sub protocol
- Multiple QOS (Quality of Service) levels
  - QOS 0 – No ack from the server, receive at most once
  - QOS 1 – Server acks packet, receive at least once
  - QOS 2 – Receive exactly once

MQTT Demo

```
$ mosquito

$ mosquitto_sub --topic /home/+/temperature -v

$ mosquitto_pub --topic /home/living_room/temperature -m "60"
```

Lightweight Machine to Machine (LwM2M)

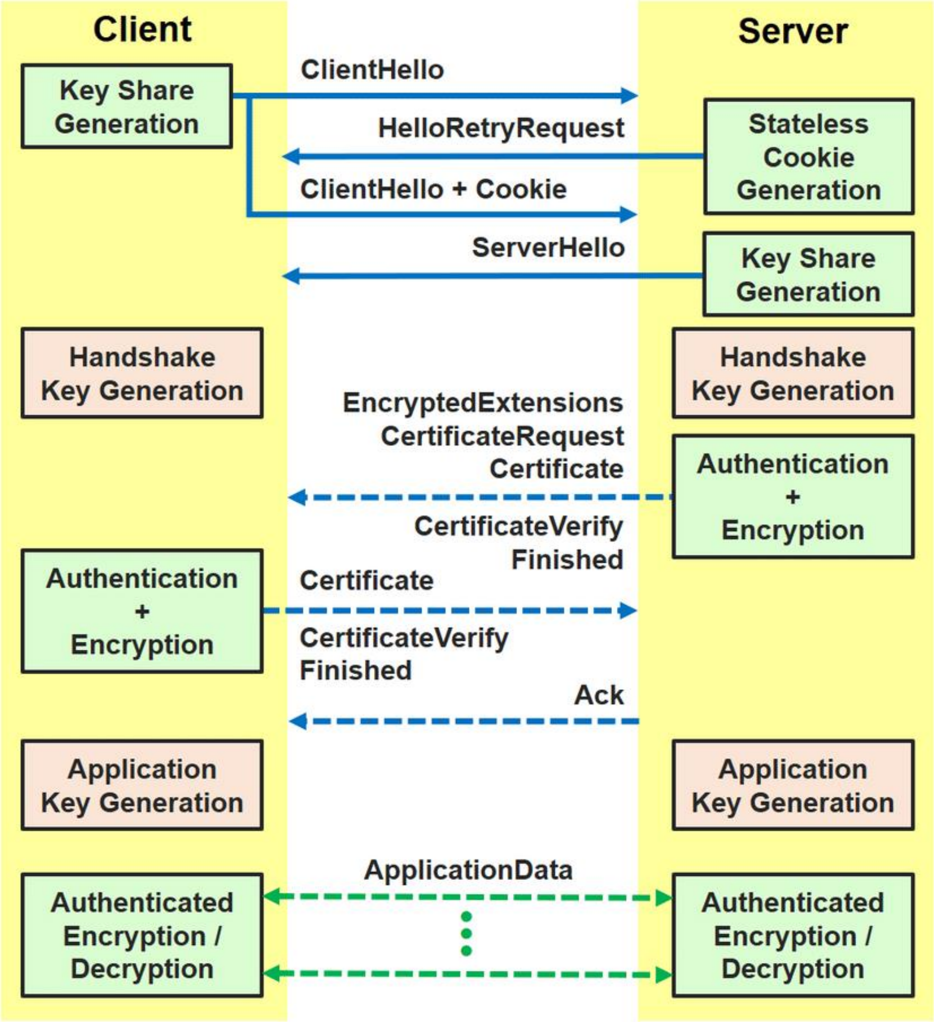
- Use for management of low resource devices
  - Bootstrap device management
  - Device configuration
  - Firmware Update
  - Fault Management
  - Configuration & Control
  - Reporting
- Based on top of CoAP + DTLS or OSCORE security layers
- New versions also have support for additional transport protocols (MQTT and HTTP)

Transport Layer Security (TLS)

- Offers Confidentiality and Integrity for transmitted packets
- Typically a shared secret is generated using Ephemeral Diffie-Helman key exchange which is used to encrypt packets
- Ephemeral means that a temporary key is generated for each connection (to provide forward secrecy)
  - Can these constrained devices generate keys frequently?
  - Do they have space to store the keys?
- TLS tends to be an expensive protocol

TLS vs DTLS

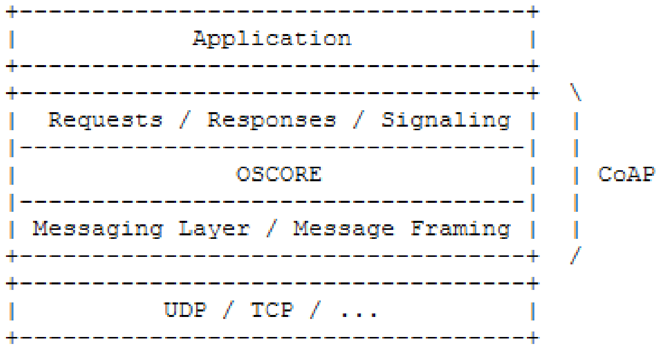
- Using TCP might be too expensive for some cyber physical systems
- Instead UDP might be preferred
- Important to still provide confidentiality
- DTLS is TLS for datagram packets (UDP packets)



U. Banerjee, C. Juvekar, S. H. Fuller and A. P. Chandrakasan, "eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8255053.

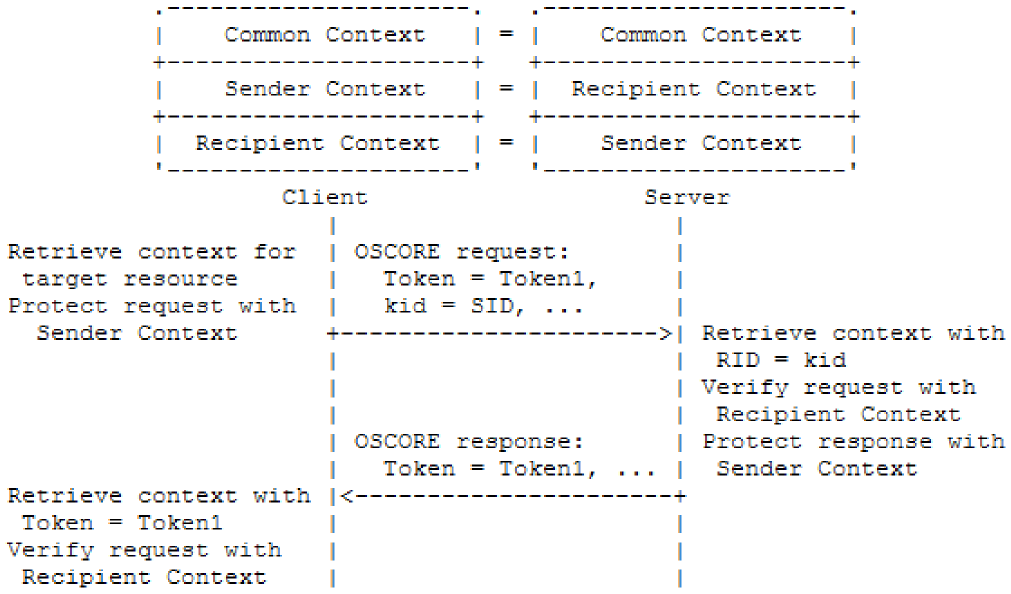
OSCORE

- A security layer specific to CoAP
- Provides Confidentiality and Integrity protection
- Intended to NOT protect all information in CoAP headers
- When routing through a proxy this information can change



```
+-----------------------------------+
|            Application            |
+-----------------------------------+
+-----------------------------------+  \
| Requests / Responses / Signaling  |  |
|-----------------------------------|  |
|              OSCORE               |  | CoAP
|-----------------------------------|  |
| Messaging Layer / Message Framing |  |
+-----------------------------------+  /
+-----------------------------------+
|           UDP / TCP / ...         |
+-----------------------------------+
```

Figure 1: Abstract Layering of CoAP with OSCORE



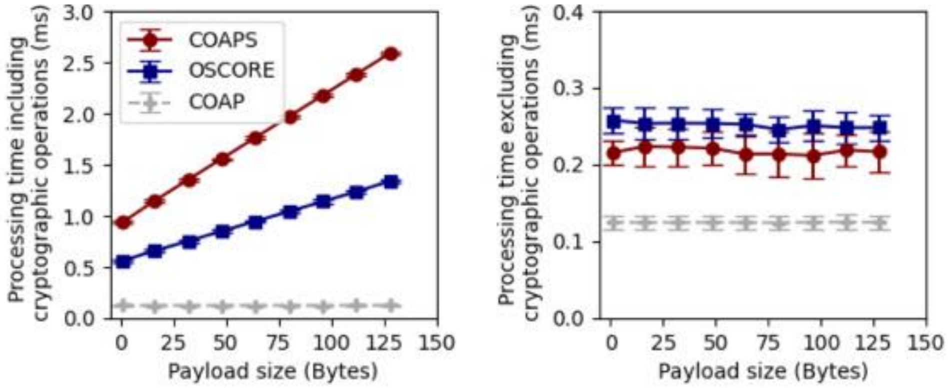
```
          .------------------------.     .------------------------.
          |     Common Context     |  =  |     Common Context     |
          +------------------------+     +------------------------+
          |     Sender Context     |  =  |   Recipient Context    |
          +------------------------+     +------------------------+
          |   Recipient Context    |  =  |     Sender Context     |
          '------------------------'     '------------------------'
                    Client                         Server
                       |                             |
Retrieve context for   | OSCORE request:             |
 target resource       |   Token = Token1,           |
Protect request with   |   kid = SID, ...            |
 Sender Context        +---------------------------->| Retrieve context with
                       |                             |  RID = kid
                       |                             | Verify request with
                       |                             |  Recipient Context
                       | OSCORE response:            | Protect response with
                       |   Token = Token1, ...       |  Sender Context
Retrieve context with  |<----------------------------+
 Token = Token1        |                             |
Verify request with    |                             |
 Recipient Context     |                             |
```

Figure 4: Retrieval and Use of the Security Context

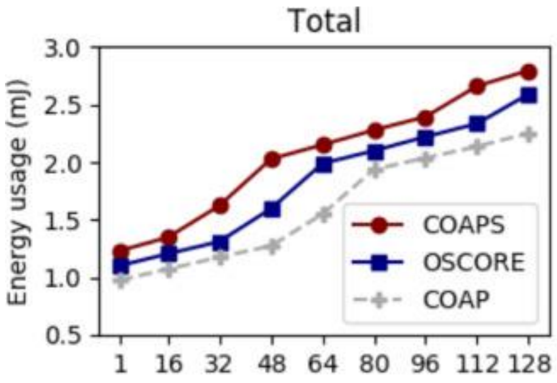
https://datatracker.ietf.org/doc/html/rfc8613

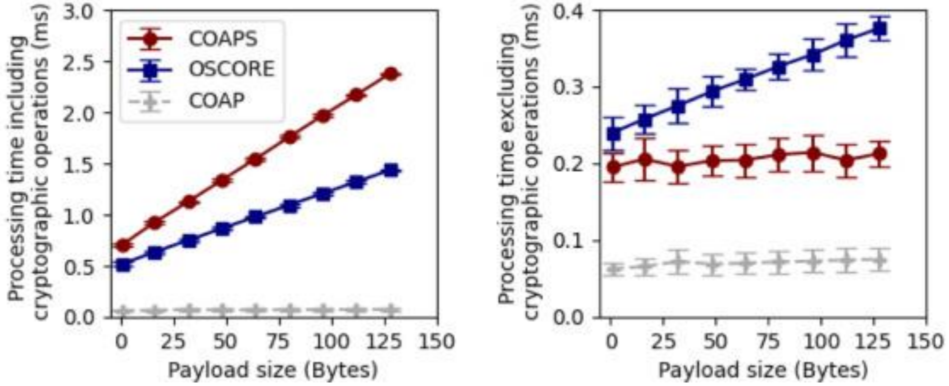
OSCORE vs DTLS

- CoAP over DTLS is slightly more expensive than OSCORE in terms of:
  - Latency
  - ROM usage
  - CPU usage
  - Network
  - Energy



(a) Measurement of CPU time when processing incoming messages with COAP, COAPS and OSCORE.

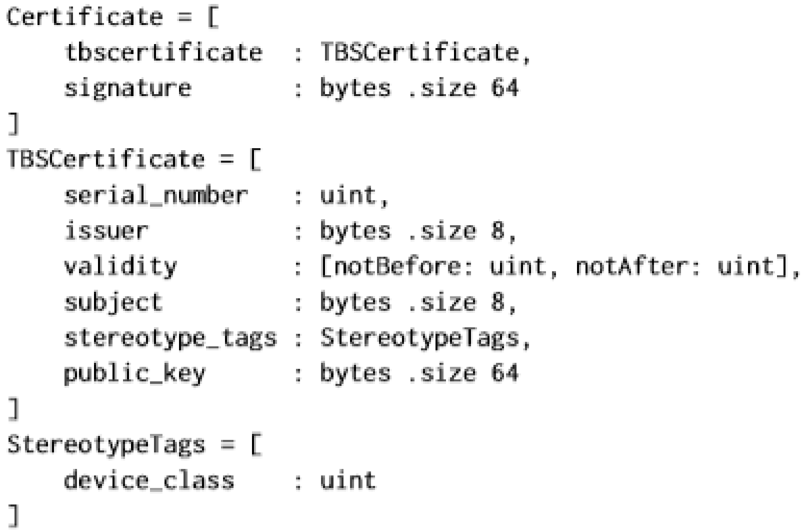




M. Gunnarsson, J. Brorsson, F. Palombini, L. Seitz, M. Tiloca. Evaluating the performance of the OSCORE security protocol in constrained IoT environments. 2021. Internet of Things, Volume 13, DOI: 10.1016/j.iot.2020.100333.

Encoding messaging - CBOR

- Text-based protocols (XML, JSON, YAML, ...) tend to have large payload sizes
- Existing binary protocols are not particularly efficient (ASN.1)
- CBOR encapsulates a stream of data where each data item has a potentially different type
- Support for:
  - Numeric types: Integers, floating point
  - Containers: sequences and mappings
  - Strings of text and bytes
  - User defined tags for objects (IP address, date, time, ...)



```
Certificate = [
    tbscertificate   : TBSCertificate,
    signature        : bytes .size 64
]
TBSCertificate = [
    serial_number    : uint,
    issuer           : bytes .size 8,
    validity         : [notBefore: uint, notAfter: uint],
    subject          : bytes .size 8,
    stereotype_tags  : StereotypeTags,
    public_key       : bytes .size 64
]
StereotypeTags = [
    device_class     : uint
]
```

https://datatracker.ietf.org/doc/html/rfc8949

CBOR Encoding Example

JSON (29 bytes)

```
{
         "hello": 1,
         "world": [1, 2, 3, 4]
}
```

- A saving of 9 bytes is a reduction of 31%
- Potential for large savings over time as many messages are sent
- Simpler to parse, smaller ROM cost
- CBOR is not human readable

CBOR (20 bytes)

```
81                  # array(1)
   A2               # map(2)
      65            # text(5)
         68656C6C6F # "hello"
      01            # unsigned(1)
      65            # text(5)
         776F726C64 # "world“
84            # array(4)
         01         # unsigned(1)
         02         # unsigned(2)
         03         # unsigned(3)
         04         # unsigned(4)
```

https://cbor.me/

OTA Firmware Update

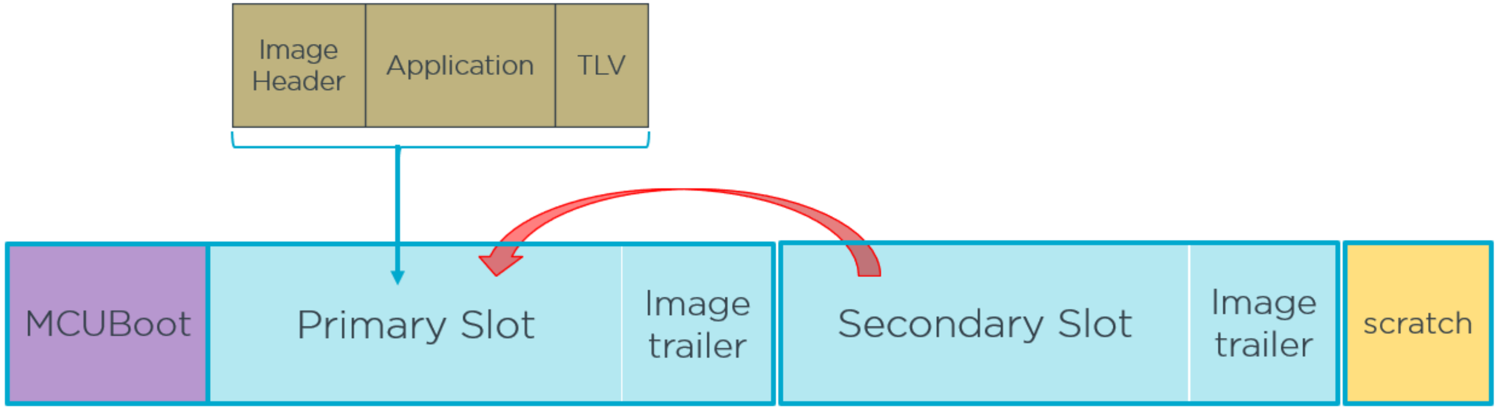
- UK’s Code of Practise for consumer IoT security #3 “Keep Software Updated”
- Updating embedded systems is hard

1. Limited resources to store new firmware
2. Limited bandwidth means slow updates
3. On battery powered devices, can only perform a few updates due to the energy cost
4. Availability impact of performing the update

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security#keep-software-updated

OTA Firmware Update

- Many approaches to improve the state of OTA updates
- IETF standardising firmware packaging with SUIT
- Encrypted firmware deployments
- Introduction of bootloaders as a separate component



https://datatracker.ietf.org/wg/suit/about/

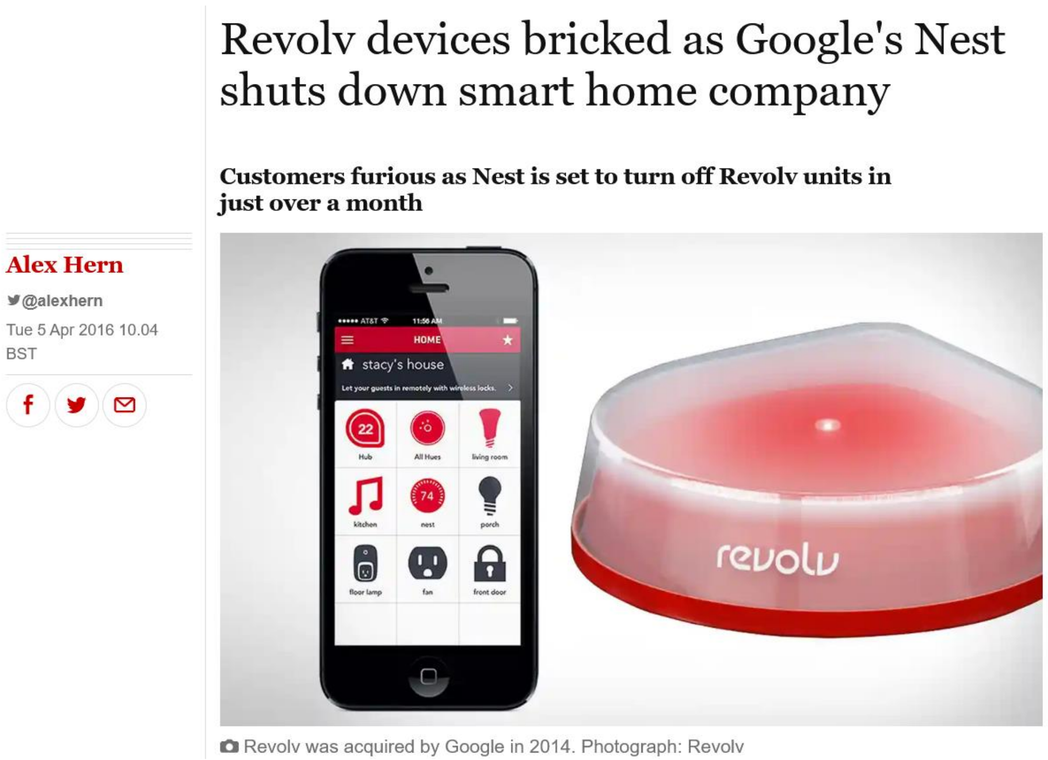
Controlling the network

- Where do you control the IoT network from?
  - Cloud
    - AWS
    - Google Cloud
    - Azure
    - …
  - Local
- Advantages / disadvantages

openHAB
empowering the smart home

thingsquare

Challenges with centralised control in the cloud



Revolv devices bricked as Google's Nest shuts down smart home company

Customers furious as Nest is set to turn off Revolv units in just over a month

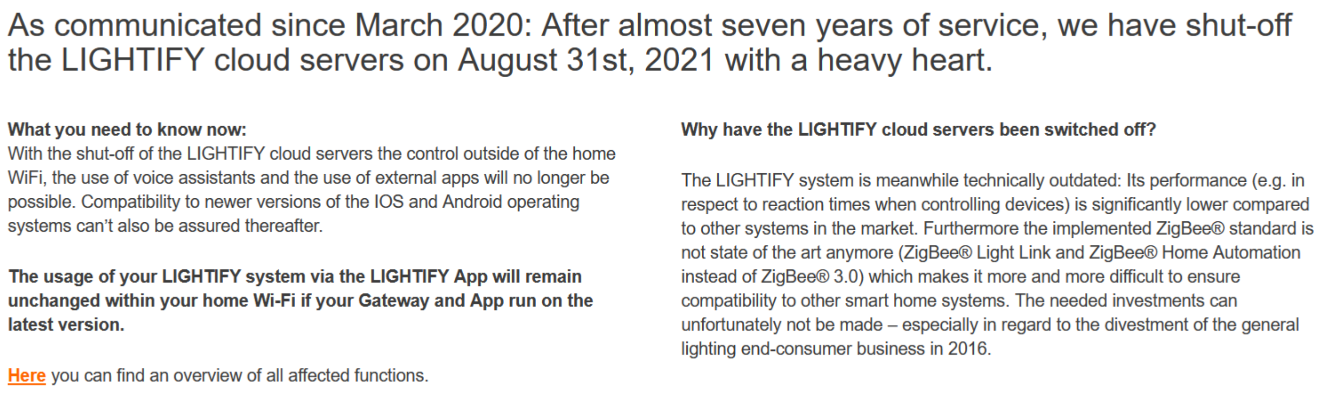
Alex Hern

@alexhern

Tue 5 Apr 2016 10.04 BST

Revolv was acquired by Google in 2014. Photograph: Revolv

https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home



As communicated since March 2020: After almost seven years of service, we have shut-off the LIGHTIFY cloud servers on August 31st, 2021 with a heavy heart.

What you need to know now:
With the shut-off of the LIGHTIFY cloud servers the control outside of the home WiFi, the use of voice assistants and the use of external apps will no longer be possible. Compatibility to newer versions of the IOS and Android operating systems can't also be assured thereafter.

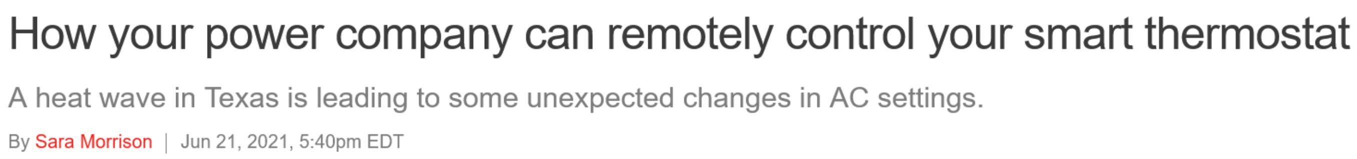
The usage of your LIGHTIFY system via the LIGHTIFY App will remain unchanged within your home Wi-Fi if your Gateway and App run on the latest version.

Here you can find an overview of all affected functions.

Why have the LIGHTIFY cloud servers been switched off?

The LIGHTIFY system is meanwhile technically outdated: Its performance (e.g. in respect to reaction times when controlling devices) is significantly lower compared to other systems in the market. Furthermore the implemented ZigBee® standard is not state of the art anymore (ZigBee® Light Link and ZigBee® Home Automation instead of ZigBee® 3.0) which makes it more and more difficult to ensure compatibility to other smart home systems. The needed investments can unfortunately not be made – especially in regard to the divestment of the general lighting end-consumer business in 2016.

https://www.osram.com/cb/lightify/index.jsp



How your power company can remotely control your smart thermostat

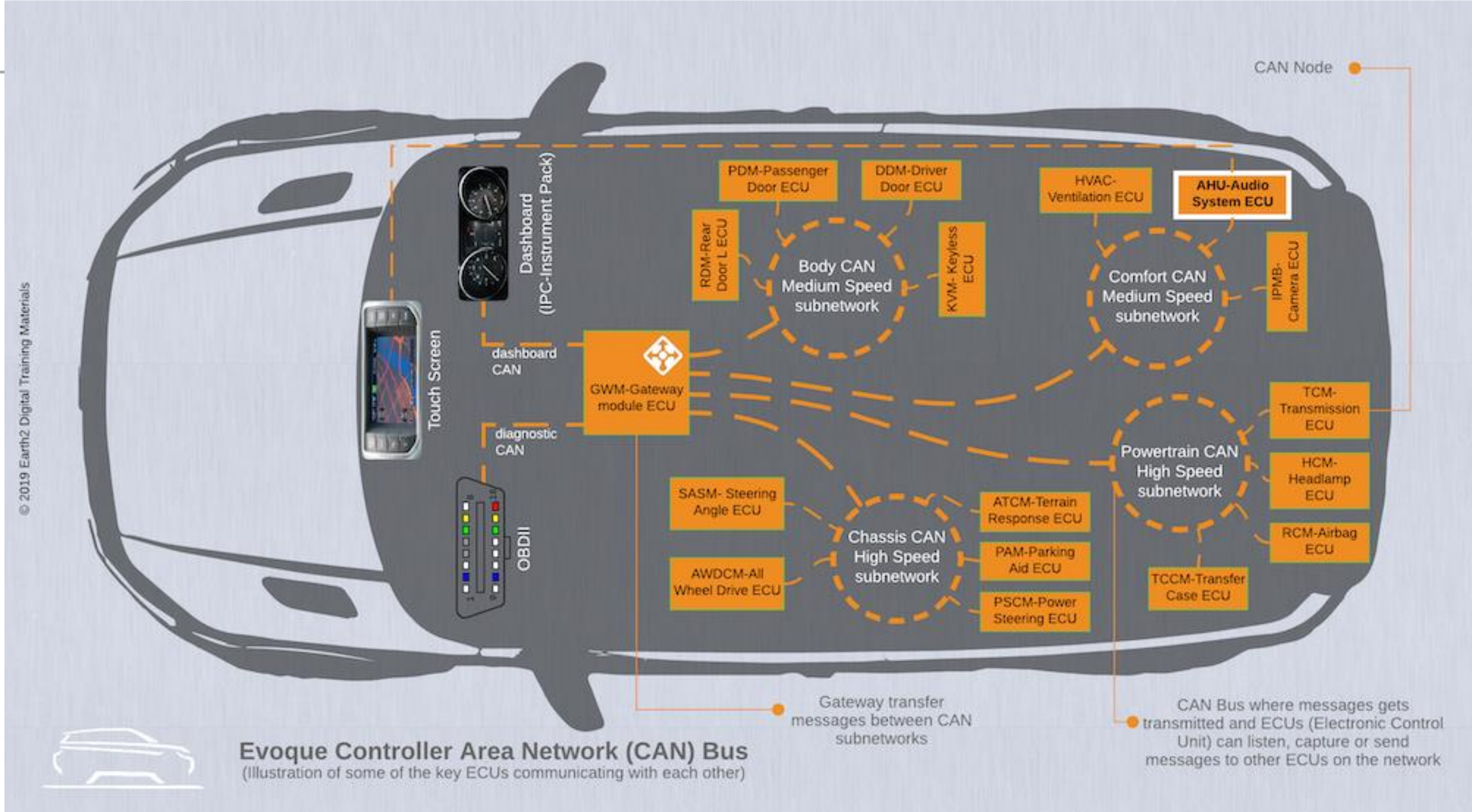
A heat wave in Texas is leading to some unexpected changes in AC settings.

By Sara Morrison | Jun 21, 2021, 5:40pm EDT

https://www.vox.com/recode/22543678/smart-thermostat-air-conditioner-texas-heatwave

Vehicles

CAN Bus Internal network


CAN Node
Dashboard
(IPC-Instrument Pack)
Touch Screen
dashboard CAN
diagnostic CAN
OBDII
GWM-Gateway module ECU
PDM-Passenger Door ECU
DDM-Driver Door ECU
RDM-Rear Door L ECU
KVM- Keyless ECU
Body CAN Medium Speed subnetwork
HVAC- Ventilation ECU
AHU-Audio System ECU
IPMB- Camera ECU
Comfort CAN Medium Speed subnetwork
TCM- Transmission ECU
HCM- Headlamp ECU
RCM-Airbag ECU
TCCM-Transfer Case ECU
Powertrain CAN High Speed subnetwork
SASM- Steering Angle ECU
AWDCM-All Wheel Drive ECU
ATCM-Terrain Response ECU
PAM-Parking Aid ECU
PSCM-Power Steering ECU
Chassis CAN High Speed subnetwork
Gateway transfer messages between CAN subnetworks
CAN Bus where messages gets transmitted and ECUs (Electronic Control Unit) can listen, capture or send messages to other ECUs on the network
© 2019 Earth2 Digital Training Materials

Evoque Controller Area Network (CAN) Bus
(Illustration of some of the key ECUs communicating with each other)

https://www.earth2.digital/blog/what-is-vehicle-can-bus-ecu-evoque-adam-ali.html

CAN Bus - Historical

- Historically no encryption or authentication
- CAN Bus assumed to be a walled garden
- If an adversary gets access to the bus, then they can have a large influence over a vehicle
  - Gain control over an electronic control unit (ECU) can allow attacker to influence system
  - Physical attacks to connect devices to the OBD-II port
- Potential for there to be vehicles in this state on the road that have not been updated

CAN Bus - Current

- Encryption and authentication on the bus is becoming common place
- Challenge of:
  - backwards compatibility
  - Performance impact of encryption/decryption/authentication on timing constraints

Case study 1

- Charlie Miller and Chris Valasek's remote exploitation of a Jeep Cheroke (2015)
- https://www.youtube.com/watch?v=MK0SrxBC1xs

http://illmatics.com/Remote%20Car%20Hacking.pdf

Case study 2

- Nie et al. Free-fall: Hacking Tesla From Wireless To CAN Bus. 2017

1. Tesla connected to unsecured WiFi hotspot by default
2. Malicious WiFi uses the same SSID
3. Car loads website by default, malicious WiFi sends webpage with malicious code to take advantage of vulnerability in car’s browser
4. Disassembling an ECU gave access to debug documentation which described firmware upgrades
5. Privilege escalation exploited to flash custom firmware on car

Mitigations:

- Fix browser vulnerability
- Remove debug information from deployment
- Digitally sign firmware to prevent execution of untrusted code

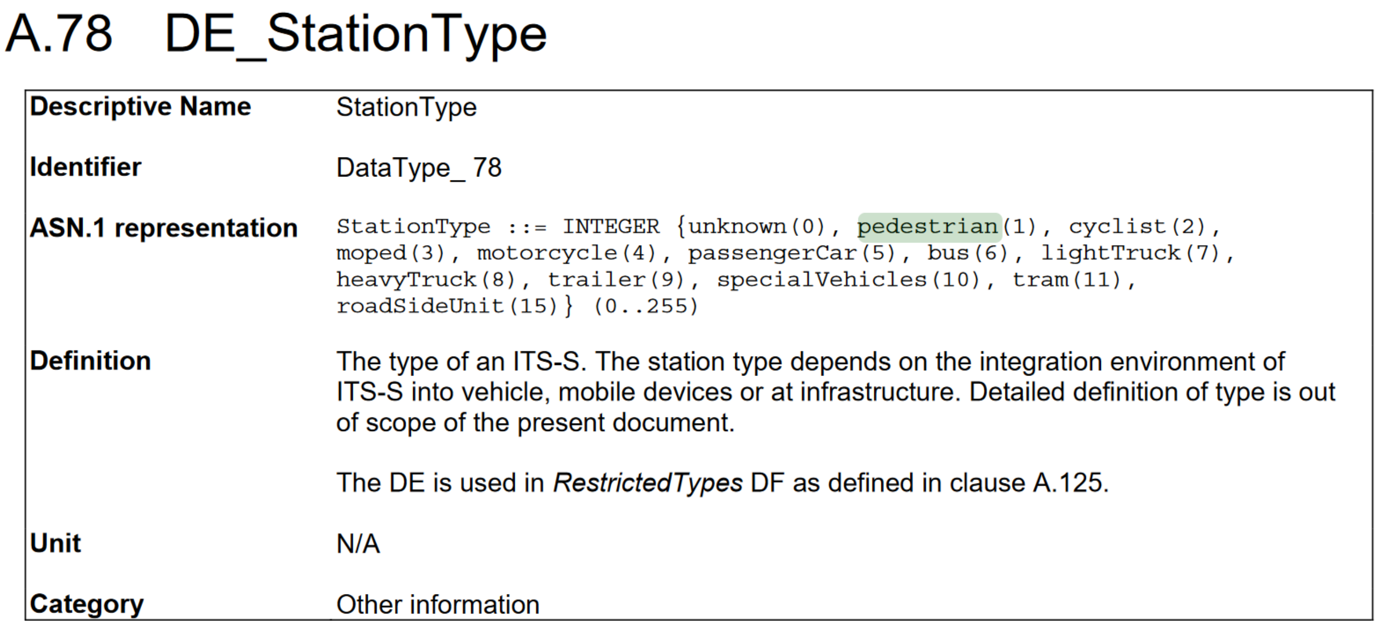
https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

Vehicles are no longer isolated networks

- Vehicles make use of wide variety of wired and wireless communications
- Wired
  - USB / HDMI / Audio ports in vehicle
  - OBD-II port
- Wireless
  - Bluetooth – local devices in the car
  - Cellular – Firmware and map updates / Road condition updates
  - Radio and DAB
  - GNSS (global navigation satellite system) e.g., GPS
  - Vehicle-to-vehicle
  - WiFi (possibly hosting an access point / possibly as a client)
  - Remote Keyless Entry

Vehicle Communication

- Vehicles communicating is a key part of
  - Connected and Autonomous Vehicles (CAV)
  - Connected and Automated Mobility (CAM)



A.78 DE_StationType

Descriptive Name	StationType
Identifier	DataType_ 78
ASN.1 representation	`StationType ::= INTEGER {unknown(0), pedestrian(1), cyclist(2), moped(3), motorcycle(4), passengerCar(5), bus(6), lightTruck(7), heavyTruck(8), trailer(9), specialVehicles(10), tram(11), roadSideUnit(15)} (0..255)`
Definition	The type of an ITS-S. The station type depends on the integration environment of ITS-S into vehicle, mobile devices or at infrastructure. Detailed definition of type is out of scope of the present document. The DE is used in *RestrictedTypes* DF as defined in clause A.125.
Unit	N/A
Category	Other information

ETSI TS 102 894-2 V1.2

Vehicle to Vehicle Communication

Why Communicate?

- Broadcast Safety Messages (CAM / BSM)
- Inform other vehicles of events (DENM)
- Manage autonomous platoons
- Logistics and freight management
- Other: Stream video between vehicles

What is in a Cooperative Awareness Message?

- Sent by a vehicle every 100-1000ms
- Contains information used to avoid unsafe scenarios (e.g., collisions)
  - GNSS coordinate
  - Speed
  - Heading
  - Acceleration

- Other useful vehicle information
  - Vehicle Dimensions
  - Light status
  - Is it carrying dangerous goods?
- Messages are intentionally unencrypted
- Protected with a digital signature for non-repudiation and integrity

ETSI EN 302 637-2 V1.4

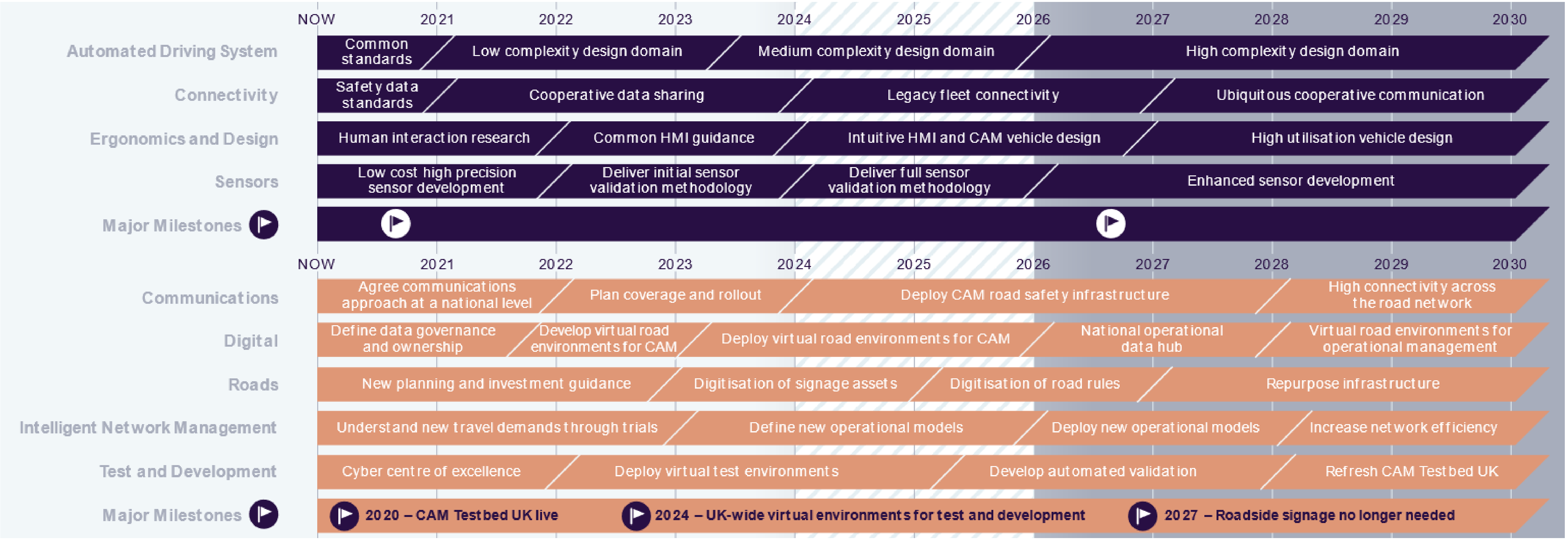
What is in a Decentralised Event Notification Message?

- Sent by a vehicle when an event occurs
- Contains information about the event
  - When and where it occurred
  - Area of relevance
  - Event duration
- DENMs can be forwarded to make other vehicles aware of the event
- Messages are intentionally unencrypted
- Protected with a digital signature for non-repudiation and integrity

- Traffic condition
- Accident
- Roadworks
- Adverse weather conditions
- Hazardous location
  - Surface conditions
  - Obstacle
  - Animal
- Human presence on road
- Wrong way driving
- …

ETSI EN 302 637-3 V1.3.1

Where are we with Vehicular Communication?



Automated Driving System
- Common standards
- Low complexity design domain
- Medium complexity design domain
- High complexity design domain

Connectivity
- Safety data standards
- Cooperative data sharing
- Legacy fleet connectivity
- Ubiquitous cooperative communication

Ergonomics and Design
- Human interaction research
- Common HMI guidance
- Intuitive HMI and CAM vehicle design
- High utilisation vehicle design

Sensors
- Low cost high precision sensor development
- Deliver initial sensor validation methodology
- Deliver full sensor validation methodology
- Enhanced sensor development

Major Milestones

Communications
- Agree communications approach at a national level
- Plan coverage and rollout
- Deploy CAM road safety infrastructure
- High connectivity across the road network

Digital
- Define data governance and ownership
- Develop virtual road environments for CAM
- Deploy virtual road environments for CAM
- National operational data hub
- Virtual road environments for operational management

Roads
- New planning and investment guidance
- Digitisation of signage assets
- Digitisation of road rules
- Repurpose infrastructure

Intelligent Network Management
- Understand new travel demands through trials
- Define new operational models
- Deploy new operational models
- Increase network efficiency

Test and Development
- Cyber centre of excellence
- Deploy virtual test environments
- Develop automated validation
- Refresh CAM Testbed UK

Major Milestones
- 2020 – CAM Testbed UK live
- 2024 – UK-wide virtual environments for test and development
- 2027 – Roadside signage no longer needed

https://zenzic.io/content/uploads/2020/10/Zenzic_Roadmap_Report_v3.pdf

What technology will be used?

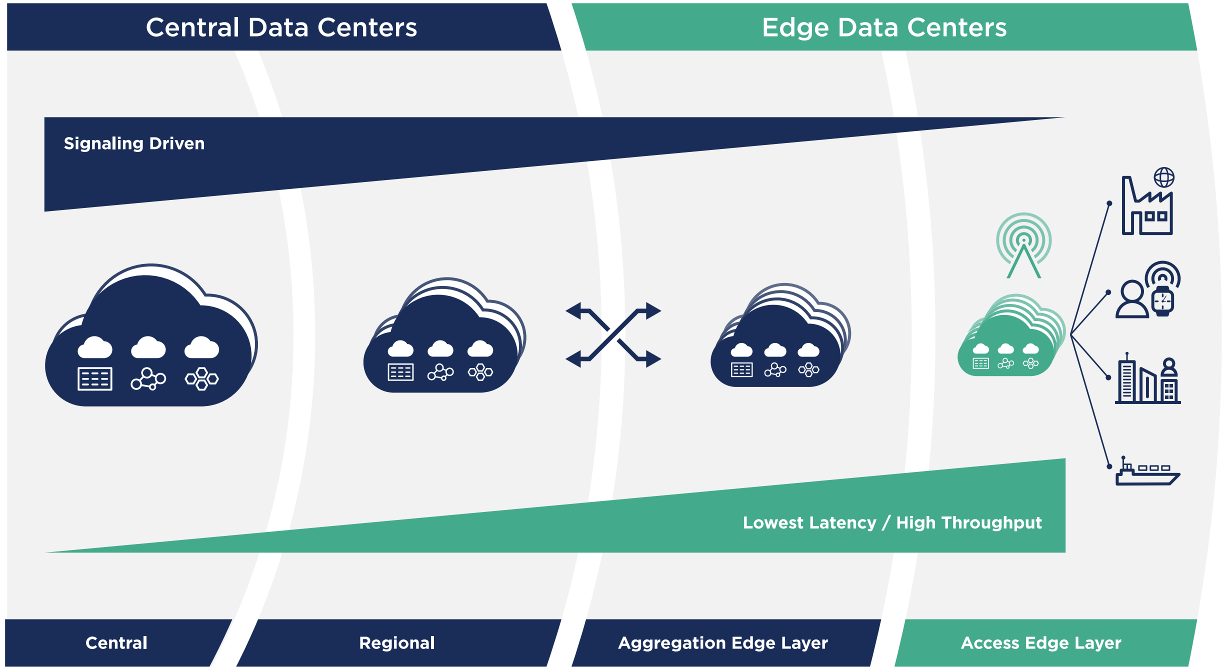
- Complicated
- Initial work used IEEE 802.11p / DSRC – based on WiFi
    - Dedicated Short Range Communication
    - Easy to do V2V
    - Good range
- But there is also interest in deploying a cellular-based technology C-V2X
- General preference for C-V2X.
- Possible Reason: If roadside infrastructure needs to be deployed every 500m – 1km along every road, why not do it with equipment that facilitates 5G?

Vehicle to Anything Communication

- Vehicles will not only communicate with other vehicles (V2V)
- Roadside infrastructure (V2I)
- Cloud (V2C)
- Pedestrians (V2P)
- Your home (V2H)
- …

Roadside Edge Infrastructure

- Some applications will be latency sensitive
- Typical: Submit task to cloud computing resources
- Alternative: Deploy compute infrastructure at the edge of a system



https://www.openstack.org/use-cases/edge-computing/edge-computing-next-steps-in-architecture-design-and-testing/

Summary

- The internet is not just clients connecting to servers hosted in a cloud
- Reality:
  - Potential for very large number of devices
  - Wide variety of different devices
  - Potential for isolated networks
  - Potential for networks that can be bridged to access wider internet
- Trend of making devices “smart” leading to additional connectivity

Lancaster University

Thank you! Questions?