CoAP EdgeX Device Service
and low power wireless

Ken Bannister
2020-10-12
About Ken

- Software Engineer, 30+ years experience
- Broad background but focus on low power wireless
- Author of gcoap library for RIOT OS
- Commercial sensor network product team
Topics

- CoAP format, stack, security
- device-coap-c integration
- Next steps
- Wireless use cases
CoAP

- Constrained Application Protocol
- IETF RFC 7252, 2014
- Compact, binary request/response
- UDP / IP

**HTTP / REST for constrained environments**
Network Stack

- 127 byte frame
- mesh network, sensors, lighting, Nest
- Nordic, TI, ST, NXP, SiLabs, Microchip
- CHIP – Connected Home over IP (Zigbee, Thread, BLE) Amazon, Apple, Google

https://openthread.io/platforms/
EdgeX for Wireless Sensors

- Segregate NB/SB networking
  - HTTP/MQTT (TCP) <-- CoAP (UDP)
  - IPv4 <-- IPv6
  - TLS <-- Link layer
- Aggregate sensor network data for NB
- Fuse sensor data into local actions
Message Format

Type | 0 CONfirmable, 1 NON-confirmable, … reliability
---|---
Code | 0.1 GET, 0.2 POST, … 2.05 Content, 4.04 Not Found
Message ID | Deduplication
Token | Up to 8 bytes, transaction management
Options | 11 Uri-Path, 12 Content-Format, … delta encoding
Payload | Block protocol if not big enough

Link Layer Security

- 802.15.4 AES-CCM, like DTLS PSK
- Thread
- EdgeX at wireless border
CoAP Transport Security

DTLS for UDP

- Pre-shared Key – AEC-CCM 16 bytes
- Full certificate or raw public key
- TinyDTLS, MbedTLS, OpenSSL, WolfSSL, GnuTLS
- See RFC 7925
OSCORE Security

- Application level, end to end
- Payload and some options
- 2019
device-coap-c

- async data post, like *device-rest-go*
- libcoap - mature
- DTLS PSK security
- GitHub: kb2ma/device-coap-c
Device–Service Mapping

- `deviceName` – pre-defined in service config
- `resourceName` - same for device and service
Demo Time!

- Adafruit ESP8266 + MCP9808 I2C temperature sensor
- riot-edgex-coap-client firmware
- README, profile, config
Next Steps

- EdgeX site link to device-coap-c repo?
- More data types
- Vault credentials
- Device specific authentication

Long term: LwM2M

- Device registration, configuration
CoAP by Wireless Range

Low power, IP, low latency, mesh networks

https://link.springer.com/chapter/10.1007/978-3-030-36625-4_42
LAN - 6TiSCH and IIOT

- IPv6 + Time slotted channel hopping
- TSCH = 802.15.4e, WirelessHART, ISA 100
- Mesh networks, high reliability, low power
- Analog Devices (Dust), Cisco
MAN - Wi-SUN

FAN Use Cases

Network Operations Center

Public or Private WAN Backhaul
(Cellular, WiMAX, Fiber/Ethernet)

IEEE 802.15.4/e RF Mesh

IEEE 802.15.4/e RF Mesh

IEEE 802.15.4/e RF Mesh

AMI Metering
Transformer Monitoring
Distribution Automation
EV Charging Infrastructure
Direct Load Control
Outdoor Lighting
Gas / Water Meters
Distributed Generation
SCADA Protection and Control Network

Smart Grid – Itron, Landis+Gyr
Smart City – City of London, Copenhagen, Tokyo

WAN – LwM2M, NB-IoT

- **LwM2M** – OMA application spec
- Generic, end-to-end solution
- Bootstrap server, Queue mode, ...
- Path `/3303/{n}/5700 = temperature value`
- **NB-IoT** – long range, no mesh
- **NIDD** – non-IP transport
- **T-Mobile, AT&T, Verizon, ARM Pelion, Ericsson**

Next Generation

- Scavenge energy – ambient light, heat, vibration
- Very small, implantable
- Range 10s of meters
- Presumably low cost
- Cortex M0, 16k RAM
- Validates tiered networking

https://www.cubeworks.io/product/cubisens-tc110/